



# ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ JACARTA MANAGEMENT SYSTEM 4LX

Руководство администратора. Часть 1

Установка и настройка

Инв. № подл.	Подп. и дата
Взам. инв. №	Инв. № дубл.
Подп. и дата	Подп. и дата

Версия продукта	4LX
Версия документа	1.02
Статус	Публичный
Дата	16 апреля 2024 г.
Листов	116

# Оглавление

1.	О документе	7
1.1	Назначение документа	7
1.2	На кого ориентирован данный документ	7
1.3	Соглашения по оформлению	7
1.4	Обозначения и сокращения	8
1.5	Авторские права, товарные знаки, ограничения	10
1.6	Лицензионное соглашение	11
2.	Введение	14
2.1	Приемка изделия	14
2.2	Общие сведения	14
2.3	Состав JMS	14
3.	Описание пакета установки	15
4.	Системные требования	16
5.	Установка и первоначальная настройка	16
5.1	Начальные условия для развертывания JMS	16
5.2	Установка и первоначальная настройка сервера и консольного агента JMS	17
5.2.1	Подготовительные действия	17
5.2.2	Установка компонентов сервера JMS	18
5.3	Установка и первоначальная настройка серверного web-приложения Консоль управления JMS (JMS Web Admin)	20
5.3.1	Подготовительные действия	20
5.3.2	Установка серверного компонента Консоли управления JMS	20
5.3.3	Проверка работы web-приложения Консоль управления JMS	22
5.3.4	Дополнительные настройки	24
5.4	Установка и первоначальная настройка JMS Web Agent (JWA)	24
5.4.1	Подготовительные действия	24
5.4.2	Установка JWA	25
5.4.3	Управление процессом JWA	27
5.4.4	Проверка работы JWA с Консолью управления JMS	27
5.5	Установка и первоначальная настройка приложения JMS Web Agent Tray	28
5.5.1	Подготовительные действия	29
5.5.2	Установка JWA Tray	29
5.6	Обеспечение поддержки СДР ALO на клиентских компьютерах	30
6.	Активация продукта	30
7.	Порядок обновления компонентов JMS	34

7.1	Остановка служб компонентов JMS	34
7.2	Резервное копирование БД JMS	35
7.3	Удаление компонентов JMS	35
7.4	Установка новой версии сервера JMS (в рамках обновления продукта)	35
7.5	Обновление БД JMS	35
7.6	Установка остальных компонентов JMS (в рамках обновления продукта)	35
7.7	Запуск и проверка работоспособности компонентов JMS	36
8.	Журналы диагностики JMS	36
9.	Обеспечение целостности и защиты от несанкционированного доступа файлов ПО JMS	36
10.	Настройка функций безопасности среды функционирования объекта оценки (JMS)	36
11.	Установка и настройка плагина СКЗИ «Крипто БД» для JMS	36
12.	Утилита сбора диагностической информации о JMS	42
13.	Сведения по запуску планов обслуживания из консольного агента JMS	44
13.1	Автоматическая организация очередей выполнения заданий планов обслуживания	44
13.2	Настройка автоматического регулярного запуска планов обслуживания	45
13.2.1	Пример добавления задания в crontab на выполнение плана обслуживания	45
13.3	Автоматическая генерация параметров запуска команды maintenance run	46
14.	Добавление поддержки моделей ЭК / профилей в JMS	48
15.	Установка коннектора к Offline Certification Authority	48
15.1	Дистрибутив	49
15.2	Системные требования коннектора к Offline Certification Authority	49
15.3	Порядок установки коннектора к Offline Certification Authority	49
15.3.1	Подготовительные действия	49
15.3.2	Установка	49
15.4	Порядок удаления коннектора к Offline Certification Authority	51
16.	Установка Прокси-сервера для УЦ (Web API к УЦ)	51
16.1	Дистрибутив	52
16.2	Системные требования Прокси-сервера для УЦ MSCA	52
16.3	Порядок установки Прокси-сервера для УЦ MSCA	52
16.3.1	Подготовительные действия	52
16.3.2	Установка	52
16.4	Первичная проверка работы Прокси-сервера для УЦ MSCA	54
16.5	Настройки Прокси-сервера для УЦ MSCA	54

16.6	Настройка подключения к УЦ	54
16.7	Настройка полномочий на MSCA для доменного компьютера – прокси-сервера	54
16.8	Настройка адресов и портов	55
16.9	Настройка SSL	55
16.10	Настройка аутентификации и авторизации	55
16.11	Настройка локализации	56
16.12	Настройка работы прокси на клиентских операционных системах	56
16.13	Журналы диагностики Прокси-сервера для УЦ MSCA	56
16.14	Настройка сервера JMS для работы с Прокси-сервером для УЦ MSCA	57
17.	Подготовка к использованию протоколов SSL/TLS	58
17.1	Настройка SSL-соединения на стороне сервера JMS	58
17.2	Настройка SSL/TLS на стороне Web-приложения Консоль управления JMS	59
17.3	Настройка SSL/TLS на стороне web-клиента JMS	60
17.4	Настройка SSL/TLS для работы с СУБД	61
17.4.1	Настройка SSL/TLS для работы с СУБД на стороне сервера JMS	61
17.4.2	Настройка SSL/TLS для работы с MS SQL	61
17.4.3	Настройка SSL/TLS для работы с PostgreSQL	62
17.5	Настройка SSL для доступа к ресурсной системе	63
17.6	Настройка SSL в подсистеме JWM	65
18.	Порядок настройки прозрачной аутентификации доменных пользователей AD в клиентских приложениях JMS	66
19.	Настройка внутренней точки доступа к IntegrationManager API	68
20.	Компонент JMS Web Manager (JWM)	68
20.1	Дистрибутив	69
20.2	Системные требования компонентов JWM	69
20.3	Развёртывание JWM	70
20.3.1	Подготовительные действия	71
20.3.2	Установка компонентов JWM	74
20.3.3	Первоначальная настройка компонентов JWM	74
20.3.4	Подготовительные действия для самостоятельной установки JWA пользователями	75
21.	JWM-коннектор для JMS и консоли управления (JMS Web Admin)	75
21.1	Дистрибутив	75
21.2	Системные требования JWM-коннектора для JMS	76
21.3	Установка и настройка JWM-коннектора на серверах JMS и JMS Web Admin	76
Приложение 1. Параметры файла первоначальной конфигурации сервера JMS		78

Секция [service]	78
Секция [database]	78
Секция [accountSystem]	79
Секция [primaryUser]	80
Секция [licenses]	81
Секция [sts]	81
Секции [userProperty]	81
Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal	83
Команда a2fa	83
Команда accountsystem	84
Команда applet	85
Команда binding	85
Команда certificates	86
Команда connector	87
Команда cryptodb	87
Команда jas	88
Команда jwm	88
Команда jwt	89
Команда licenses	89
Команда maintenance	91
Команда server	92
Команда smtp	95
Команда ssl	96
Команда syslog	97
Команда userproperty	97
Приложение 3. Инструкция по сборке расширения rjjava для СУБД PostgreSQL 9.6 под ОС Astra Linux	100
Приложение 4. Справочник команд коннектора к Offline Certification Authority	104
Приложение 5. Справочник команд JMS Web Agent (JWA)	106
Приложение 6. Порядок генерации файла keytab для прозрачной аутентификации в JMS пользователей из домена AD по протоколу Kerberos	107
Приложение 7. Параметры файла первоначальной конфигурации компонентов сервера JWM	108
Секция [userplace]	108
Секция [jwm]	108
Секция [cors ]	109

Секция [jwa]	109
Секция [dataservice]	109
Секция [authservice]	110
Секция [jms]	110
Секция [jas]	111
Секция [database]	111
Секция [jwt ]	111
Контакты, техническая поддержка	113
Список литературы	114
Регистрация изменений	115

# 1. О документе

## 1.1 Назначение документа

Настоящий документ является частью руководства администратора и представляет собой описание операций по установке и настройке системы управления средствами аутентификации и защищенными носителями информации JaCarta Management System 4LX для среды функционирования Linux (далее – JMS).





## 1.2 На кого ориентирован данный документ

Документ предназначен для администраторов корпоративной информационной системы управления средствами аутентификации.

## 1.3 Соглашения по оформлению


В данном документе для представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице 1.

Табл. 1 – Элементы оформления

<b>Выделение</b>	Используется для выделения наименований полей, кнопок, секций, вкладок экранных форм
<code>file.exe</code>	Используется для выделения имен файлов, каталогов, текстов программ
[1]	Ссылка на пункт в списке литературы (приведен в конце документа)
<a href="#">Гиперссылка</a>	Используется для выделения внешних ссылок
Ссылка, с. 7	Используется для выделения перекрестных ссылок
	Важная информация
	Ссылка, примечание, заметка
	Совет
	Рекомендация

## 1.4 Обозначения и сокращения

Табл. 2– Обозначения и сокращения

<b>JMS</b>	То же, что «Программное обеспечение JaCarta Management System 4LX»
<b>JMS Web Admin</b>	Серверное web-приложение Консоль управления JMS
<b>JWA (JMS Web Agent)</b>	Программное обеспечение, обеспечивающее взаимодействие web-клиента JMS с ЭК/ЗНИ/СДР из среды web-браузера.
<b>JWA Tray (JMS Web Agent Tray)</b>	Программа, позволяющая выполнять базовые операции с ЭК/ЗНИ/СДР пользователя в фоновом режиме или через простое графическое меню. Запущенное приложение отображается значком  в области уведомлений рабочего стола
<b>PIN-код администратора</b>	Секретная последовательность, известная только администратору, которую необходимо предъявить для аутентификации администратора в приложении электронного ключа
<b>PIN-код подписи (PIN-код ЭП)</b>	Секретная последовательность, известная только пользователю, которую необходимо предъявить для выполнения операции электронной подписи
<b>PIN-код пользователя</b>	Секретная последовательность, известная только пользователю, которую необходимо предъявить для аутентификации пользователя в приложении электронного ключа
<b>USB</b>	Universal Serial Bus, универсальная последовательная шина
<b>web-клиент JMS</b>	Web-приложение Клиент JMS.  Комплекс программ, состоящий из компонента JMS Web Agent из комплекта поставки ПО JMS и web-клиента, функционирующего в среде web-браузера
<b>ALO, СДР ALO</b>	<b>Aladdin LiveOffice</b> – средство обеспечения безопасной дистанционной работы (СДР) компании Аладдин. В качестве электронного ключа (USB-носителя) использует устройство Aladdin LiveToken (далее для простоты – <b>СДР ALO</b> )
<b>ЗНИ</b>	Защищенный носитель информации – электронный ключ JaCarta SF/ГОСТ, обеспечивающий гарантированную защиту информации, хранимую во внутренних разделах электронного ключа (скрытые разделы RW и CD-ROM)
<b>КД</b>	Ключевой документ – в терминологии JMS это ключевая информация (КИ), записанная на электронный ключ (ключевой носитель – СКЗИ) и хранящаяся на нем
<b>КИ</b>	Ключевая информация – в терминах JMS это сертификат открытого ключа и соответствующий данному сертификату закрытый ключ (Номер КИ – это серийный номер сертификата открытого ключа)
<b>Клиентский агент</b>	То же, что приложение <b>Клиент JMS</b> . Приложение с графическим пользовательским интерфейсом, предназначенное управления электронными ключами на рабочих станциях конечных пользователей.
<b>Консольный агент</b>	Приложение, предназначенное для конфигурирования сервера JMS. Устанавливается вместе с компонентом JMS Server



<b>НД</b>	Нормативный документ – в терминах JMS означает вид документов (актов), формируемых при операциях с СКЗИ в соответствии с требованиями регулятора
<b>ПО</b>	Программное обеспечение
<b>СДР</b>	Средство дистанционной работы пользователей с вычислительными и информационными ресурсами автоматизированной (информационной) системы
<b>СКЗИ</b>	Средство криптографической защиты информации
<b>ФКН</b>	Функциональный ключевой носитель
<b>ФСБ</b>	Федеральная служба безопасности Российской Федерации
<b>ФСТЭК</b>	Федеральная служба по техническому и экспортному контролю Российской Федерации
<b>ЭК</b>	Электронный ключ – электронное устройство, используемое как средство аутентификации, и/или защищенного хранения информации, и/или USB-носитель СДР

## 1.5 Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации.

Обладателем исключительных авторских и имущественных прав является АО «Аладдин Р. Д.».

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на АО «Аладдин Р. Д.» обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является АО «Аладдин Р. Д.».

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

### Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р. Д.» без предварительного уведомления.

АО «Аладдин Р. Д.» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

АО «Аладдин Р. Д.» не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование

программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р. Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

АО «Аладдин Р. Д.» НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р. Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

### Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и резспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

## 1.6 Лицензионное соглашение

ВАЖНО:

ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ, ПРЕЖДЕ ЧЕМ ОТКРЫТЬ ПАКЕТ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ И/ИЛИ ИСПОЛЬЗОВАТЬ ЕГО СОДЕРЖИМОЕ И/ИЛИ ПРЕЖДЕ, ЧЕМ ЗАГРУЖАТЬ ИЛИ УСТАНОВЛИВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

ВСЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ НАСТОЯЩЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (включая без ограничений библиотеки, утилиты, файлы для скачивания с Web-сайта, CD-ROM, Руководства, описания и др. документацию), далее «ПО», «Продукт»), ПРЕДОСТАВЛЯЕМЫЕ КОМПАНИЕЙ АО «Аладдин Р.Д.» (или любым дочерним предприятием – каждое из них упоминаемое как «КОМПАНИЯ») ПОДЧИНЯЮТСЯ И БУДУТ ПОДЧИНЯТЬСЯ УСЛОВИЯМ, ОГОВОРЕННЫМ В ДАННОМ СОГЛАШЕНИИ.

ОТКРЫВАЯ ПАКЕТ, СОДЕРЖАЩИЙ ПРОДУКТ И/ИЛИ ЗАГРУЖАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ как определено далее по тексту) И/ИЛИ УСТАНОВЛИВАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШ КОМПЬЮТЕР И/ИЛИ ИСПОЛЬЗУЯ ДАННЫЙ ПРОДУКТ, ВЫ ПРИНИМАЕТЕ ДАННОЕ СОГЛАШЕНИЕ И СОГЛАШАЕТЕСЬ С ЕГО УСЛОВИЯМИ.

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С ДАННЫМ СОГЛАШЕНИЕМ, НЕ ОТКРЫВАЙТЕ ЭТОТ ПАКЕТ И/ИЛИ НЕ ЗАГРУЖАЙТЕ И/ИЛИ НЕ УСТАНОВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕЗАМЕДЛИТЕЛЬНО (не позднее 7 дней с даты получения этого пакета) ВЕРНИТЕ ЭТОТ ПРОДУКТ В АЛАДДИН Р.Д., СОТРИТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВСЕ ЕГО ЧАСТИ В СВОЕМ КОМПЬЮТЕРЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО НИКОИМ ОБРАЗОМ.

Лицензионное соглашение на использование программного обеспечения.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) - конечным пользователем (далее "Пользователь") и компанией АО «Аладдин Р.Д.» (далее «компания Аладдин Р.Д.», «Правообладатель») относительно предоставления неисключительного права на использование настоящего программного обеспечения - комплекса программ для ЭВМ, и документации (печатные материалы, носители и файлы с информацией), являющихся неотъемлемой частью ПО, включая все дальнейшие усовершенствования.

Лицензионный договор считается заключенным с момента начала использования Вами ПО любым способом или с момента, когда Вы примете все условия настоящего Лицензионного договора в процессе установки ПО. Лицензионный договор сохраняет свою силу в течение всего срока действия исключительного права на ПО, если только иное не оговорено в Лицензионном договоре или в отдельном письменном договоре между Вами и компанией Аладдин Р.Д. Срок действия Лицензионного договора также может зависеть от объема Вашей Лицензии, описанного в данном Лицензионном договоре.

Права на ПО охраняются действующими законодательством и международными соглашениями. Вы подтверждаете свое согласие с тем, что Лицензионный договор имеет такую же юридическую силу, как и любой другой письменный договор, заключенный Вами. В случае нарушения Лицензионного договора Вы можете быть привлечены в качестве ответчика.

### 1. Предмет Соглашения

- 1.1. Предметом настоящего Соглашения является передача Правообладателем конечному Пользователю неисключительного права на использование ПО. ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Все условия, оговоренные далее, относятся как к ПО в целом, так и ко всем его компонентам в отдельности. Данное соглашение не передает Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничего в данном Соглашении не подтверждает отказ компании Аладдин Р.Д. от прав на интеллектуальную собственность по какому бы то ни было законодательству.
- 1.2. Компания Аладдин Р.Д. сохраняет за собой все права, явным образом не предоставленные Вам настоящим Лицензионным договором. Настоящий Лицензионный договор не предоставляет Вам никаких прав на товарные знаки Компании Аладдин Р.Д..

- 1.3. В случае, если Вы являетесь физическим лицом, то территория, на которой допускается использование ПО, включает в себя весь мир. В случае, если Вы являетесь юридическим лицом (обособленным подразделением юридического лица), то территория на которой допускается приобретение ПО, ограничена страной регистрации юридического лица (обособленного подразделения юридического лица), если только иное не оговорено в отдельном письменном договоре между Вами и Компанией Аладдин Р.Д.

### 2. Имущественные права

- 2.1. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как "Программное обеспечение"), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остается исключительной собственностью компании Аладдин Р.Д.
- 2.2. Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтвержденные или включенные в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нем, а также все права на ПО являются и будут являться собственностью исключительно компании Аладдин Р.Д.
- 2.3. Вам, конечному Пользователю, предоставляется неисключительное право на использование ПО в указанных в документации целях и при соблюдении приведенных ниже условий.

### 3. Условия использования

- 3.1. ПО может быть использовано только в строгом соответствии с документами, инструкциями и рекомендациями Правообладателя, относящимися к данному ПО.
- 3.2. ПО может предоставляться на нескольких носителях, в том числе с помощью сети интернет. Независимо от количества носителей, на которых Вы получили ПО, Вы имеете право использовать ПО только в объеме предоставленной Вам Лицензии.
- 3.3. После уплаты Вами соответствующего вознаграждения компания Аладдин Р.Д. настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и ограниченное право на использование данного Программного обеспечения только в форме исполняемого кода, как описано в прилагаемой к Программному обеспечению документации и только в соответствии с условиями данного Соглашения:
  - ▶ Вы можете установить Программное обеспечение и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей документации компании Аладдин Р.Д.
  - ▶ Вы можете добавить/присоединить Программное обеспечение к программам Вашего компьютера с единственной целью, описанной в данном Соглашении.

Продукт должен использоваться и обслуживаться строго в соответствии с описаниями и инструкциями компании Аладдин Р.Д., приведенными в данном и других документах компании Аладдин Р.Д.

- 3.4. За исключением указанных выше разрешений, Вы обязуетесь:
  - 3.4.1. Не использовать и не выдавать сублицензии на данное Программное обеспечение и любую другую Продукцию компании Аладдин Р.Д., за исключением явных разрешений в данном Соглашении и в Руководстве по интеграции.
  - 3.4.2. Не продавать, не выдавать лицензий или сублицензий, не сдавать в аренду или в прокат, не передавать, не переводить на другие языки, не закладывать, не разделять Ваши права в рамках данного Соглашения с кем-либо или кому-либо еще.
  - 3.4.3. Не модифицировать (в том числе не вносить в ПО изменения в целях его функционирования на технических средствах Конечного пользователя), не демонтировать, не декомпилировать или дизассемблировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения.

- 3.4.4. Не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть.
- 3.4.5. Не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо еще использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.
- 3.4.6. Не пытаться обойти технические ограничения в Программе;
- 3.4.7. Не использовать Программу для оказания услуг на платной и бесплатной основе;
- 3.4.8. Не создавать условия для использования ПО лицами, не имеющими прав на использование ПО, в том числе работающими с Вами в одной многопользовательской системе или сети Интернет.
- 3.4.9. Вы не вправе удалять, изменять или делать малозаметными любые уведомления об авторских правах, правах на товарные знаки или патенты, которые указаны на/в ПО.
- 3.4.10. Вы обязуетесь соблюдать права третьих лиц, в том числе авторские права на объекты интеллектуальной собственности.
- 3.5. Компания Аладдин Р.Д. не несет обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов данного Программного обеспечения.
- Нелегальное использование, распространение и воспроизведение (копирование) программного обеспечения является нарушением действующего законодательства и преследуется по Закону.
- В случае нарушения настоящего Соглашения Правообладатель лишает Пользователя права на использование ПО. При этом Правообладатель полностью отказывается от своих гарантийных обязательств.

#### 4. Ограниченная гарантия

Компания Аладдин Р.Д. гарантирует, что:

Данное Программное обеспечение с момента поставки его Вам в течение двенадцати (12) месяцев будет функционировать в полном соответствии с Руководством Пользователя (Администратора), при условии, что оно будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Правообладатель гарантирует соответствие компонентов ПО спецификациям, а также работоспособность ПО при выполнении Пользователем условий, оговоренных в документации на ПО. ПО поставляется "таким, какое оно есть". Правообладатель не гарантирует, что ПО соответствует вашим требованиям, и что все действия ПО будут выполняться безошибочно. Правообладатель не гарантирует корректную совместную работу ПО с программным обеспечением или оборудованием других производителей.

#### 5. Отказ от гарантии

- 5.1. КОМПАНИЯ АЛАДДИН Р.Д. НЕ ГАРАНТИРУЕТ, ЧТО ЛЮБОЙ ИЗ ЕГО ПРОДУКТОВ БУДЕТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ЕГО РАБОТА БУДЕТ БЕСПЕРЕБОЙНОЙ ИЛИ БЕЗОШИБОЧНОЙ. В ОБЪЕМЕ, ПРЕДУСМОТРЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РФ, КОМПАНИЯ АЛАДДИН Р.Д. ОТКРЫТО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ, НЕ ОГОВОРЕННЫХ ЗДЕСЬ, ОТ ВСЕХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИЮ ТОВАРНОГО ВИДА И ПРИГОДНОСТИ ИСПОЛЬЗОВАНИЯ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ.
- НИ ОДИН ИЗ ДИЛЕРОВ, ДИСТРИБЬЮТОРОВ, ПРОДАВЦОВ, АГЕНТОВ ИЛИ СОТРУДНИКОВ КОМПАНИИ АЛАДДИН Р.Д. НЕ УПОЛНОМОЧЕН ПРОИЗВОДИТЬ МОДИФИКАЦИИ, РАСШИРЕНИЯ ИЛИ ДОПОЛНЕНИЯ К ДАННОЙ ГАРАНТИИ.
- 5.2. Если Вы произвели какие-либо модификации Программного обеспечения или любой из частей данного Продукта во время гарантийного периода, то гарантия, упомянутая выше, будет немедленно прекращена.
- 5.3. Гарантия недействительна, если Продукт используется на или в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в документации, или используется на компьютере с любым установленным нелегальным программным обеспечением.
- 5.4. ПО и обновления предоставляются такими, каковы они есть, и Компания Аладдин Р.Д. не предоставляет на них никаких гарантий.

Компания Аладдин Р.Д. не гарантирует и не может гарантировать работоспособность ПО и результаты, которые Вы можете получить, используя ПО.

- 5.5. За исключением гарантий и условий, которые не могут быть исключены или ограничены в соответствии с применимым законодательством, Компания Аладдин Р.Д. не предоставляет Вам никаких гарантий (в том числе явно выраженных или подразумеваемых в статутном или общем праве или обычаями делового оборота) ни на что, включая, без ограничения, гарантии о не нарушении прав третьих лиц, товарной пригодности, интегрируемости, удовлетворительного качества и годности к использованию ПО. Все риски, связанные с качеством работы и работоспособностью ПО, возлагаются на Вас.
- 5.6. Компания Аладдин Р.Д. не предоставляет никаких гарантий относительно программами для ЭВМ других производителей, которые могут предоставляться в составе ПО.

#### 6. Исключение косвенных убытков

Стороны признают, что Продукт по сути своей сложный и не может быть полностью лишен ошибок. КОМПАНИЯ АЛАДДИН Р.Д. НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ, ПОБОЧНЫЕ ИЛИ ПОТЕНЦИАЛЬНЫЕ УБЫТКИ), ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЕННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ КАКОГО-ЛИБО ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОЙ КОМПОНЕНТЫ ДАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АЛАДДИН Р.Д. ПИСЬМЕННО УВЕДОМЛЕН О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

#### 7. Ограничение ответственности

В СЛУЧАЕ ЕСЛИ, НЕСМОТЯ НА УСЛОВИЯ ДАННОГО СОГЛАШЕНИЯ, КОМПАНИЯ АЛАДДИН Р.Д. ПРИЗНАНА ОТВЕТСТВЕННОЙ ЗА УБЫТКИ НА ОСНОВАНИИ КАКИХ-ЛИБО ДЕФЕКТОВ ИЛИ НЕСООТВЕТСТВИЯ ЕГО ПРОДУКТОВ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЖДУЮ ЕДИНИЦУ ДЕФЕКТНЫХ ПРОДУКТОВ НЕ БУДЕТ ПРЕВЫШАТЬ СУММУ, ВЫПЛАЧЕННУЮ КОМПАНИИ АЛАДДИН Р.Д. ЗА ЭТИ ДЕФЕКТНЫЕ ПРОДУКТЫ.

Компания Аладдин Р.Д. ни при каких обстоятельствах не несет перед Вами никакой ответственности за убытки, вынужденные перерывы в деловой активности, потерю деловых либо иных данных или информации, претензии или расходы, реальный ущерб, а также упущенную выгоду и утраченные сбережения, вызванные использованием или связанные с использованием ПО, а также за убытки, вызванные возможными ошибками и опечатками в ПО и/или в документации, даже если Компании Аладдин Р.Д. стало известно о возможности таких убытков, потерь, претензий или расходов, равно как и за любые претензии со стороны третьих лиц. Вышеперечисленные ограничения и исключения действуют в той степени, насколько это разрешено применимым законодательством. Единственная ответственность Компании Аладдин Р.Д. по настоящему Лицензионному договору ограничивается суммой, которую Вы уплатили за ПО.

#### 8. Прекращение действия

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- (i) Лицензия, предоставленная Вам данным Соглашением, прекращает свое действие, и Вы после ее прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;
- (ii) Вы незамедлительно вернете в компанию Аладдин Р.Д. все имущество, в котором используются права Аладдин Р.Д. на интеллектуальную собственность и все копии такового и/или сотрете/удалите любую информацию, содержащуюся в них в электронном виде. Разделы 1, 3, 6-11 будут продолжать действовать даже в случае прекращения действия настоящего Соглашения.

## 9. Срок действия Договора

- 9.1. Если иное не оговорено в настоящем Лицензионном договоре либо в отдельном письменном договоре между Вами и Компанией Аладдин Р.Д., настоящий Лицензионный договор действует в течение всего срока действия исключительного права на ПО.
- 9.2. В случае нарушения вами условий настоящего Соглашения или неспособности далее выполнять его условия вы обязуетесь уничтожить все копии ПО (включая архивные, файлы с информацией, носители, печатные материалы) или вернуть все относящиеся к ПО материалы организации, в которой вы приобрели ПО. После этого Соглашение прекращает свое действие.
- 9.3. Без ущерба для каких-либо других прав Компания Аладдин Р.Д. имеет право в одностороннем порядке расторгнуть настоящий Лицензионный договор при несоблюдении Вами его условий и ограничений. При прекращении действия настоящего Лицензионного договора Вы обязаны уничтожить все имеющиеся у Вас копии ПО (включая архивные, файлы с информацией, носители, печатные материалы), все компоненты ПО, а также удалить ПО и вернуть все относящиеся к ПО материалы организации, в которой вы приобрели ПО.
- 9.4. Вы можете расторгнуть настоящий Лицензионный договор удалив ПО и уничтожив все копии ПО, все компоненты ПО и сопровождающую его документацию. Такое расторжение не освобождает Вас от обязательств оплатить ПО.

## 10. Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законами Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Применение Конвенции Организации Объединенных Наций о Договорах международной купли-продажи товаров (the United Nations Convention of Contracts for the International Sale of Goods) однозначно исключается. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

## 11. Государственное регулирование и экспортный контроль

Приобретая и/или начиная использовать Продукт, Вы обязуетесь соблюдать все применимые международные и национальные законы, которые распространяются на продукты, подлежащие экспортному контролю. Настоящее ПО не должно экспортироваться или реэкспортироваться в нарушение экспортных ограничений, имеющихся в законодательстве страны, в которой приобретено или получено ПО. Вы также подтверждаете, что применимое законодательство не запрещает Вам приобретать или получать ПО.

## 12. Программное обеспечение третьих сторон

Если Продукт содержит в себе любое программное обеспечение, предоставленное какой-либо третьей стороной, такое программное обеспечение третьей стороны предоставляется "как есть" без какой-либо гарантии, и разделы 2, 3, 6, 8, 9-12 настоящего Соглашения применяются ко всем таким поставщикам программного обеспечения и к поставляемому ими программному обеспечению, как если бы это были Аладдин Р.Д. и Продукт соответственно.

## 13. Разное

- 13.1. Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только

посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

- 13.2. Все права на материалы, не содержащиеся в ПО, но доступные посредством использования ПО, принадлежат своим законным владельцам и охраняются действующим законодательством об авторском праве и международными соглашениями. Настоящий Лицензионный договор не предоставляет Вам никаких прав на использование такой интеллектуальной собственности.
- 13.3. ПО содержит коммерческую тайну и иную конфиденциальную информацию, принадлежащую Компании Аладдин Р.Д. и третьим лицам, которая охраняется действующим законодательством Российской Федерации, международными соглашениями и законодательством страны приобретения и/или использования ПО.
- 13.4. Вы соглашаетесь на добровольную передачу Компании Аладдин Р.Д. в процессе использования и регистрации ПО своих персональных данных и выражаете свое согласие на сбор, обработку, использование своих персональных данных в соответствии с применимым законодательством, на условиях обеспечения конфиденциальности. Предоставленные Вами персональные данные будут храниться и использоваться только внутри Компании Аладдин Р.Д. и ее дочерних компаний и не будут предоставлены третьим лицам, за исключением случаев, предусмотренных применимым законодательством.
- 13.5. В случае предъявления любых претензий или исков, связанных с использованием Вами ПО Вы обязуетесь сообщить Компании Аладдин Р.Д. о таких фактах в течение трех (3) дней с момента, когда Вам стало известно об их возникновении. Вы обязуетесь совершить необходимые действия для предоставления Компании Аладдин Р.Д. возможности участвовать в рассмотрении таких претензий или исков, а также предоставлять необходимую информацию для урегулирования соответствующих претензий и/или исков в течение семи (7) дней с даты получения запроса от Компании Аладдин Р.Д.
- 13.6. Вознаграждением по настоящему Лицензионному договору признается стоимость Лицензии на ПО, установленная Компанией Аладдин Р.Д. или Партнером Компании Аладдин Р.Д., которая, подлежит уплате в соответствии с определяемым Компанией Аладдин Р.Д. или Партнером Компании Аладдин Р.Д. порядком. Вознаграждение также может быть включено в стоимость приобретенного Вами оборудования или в стоимость полной версии ПО. В случае если Вы являетесь физическим лицом, настоящий Лицензионный договор может быть безвозмездным.
- 13.7. В случае если какая-либо часть настоящего Лицензионного договора будет признана утратившей юридическую силу (недействительной) и не подлежащей исполнению, остальные части Лицензионного договора сохраняют свою юридическую силу и подлежат исполнению.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

## 2. Введение

### 2.1 Приемка изделия

Перед установкой Изделия (JMS) необходимо убедиться, что:


1. комплектность Изделия соответствует комплектности поставки, указанной в Формуляре [4];
2. на носителях информации, входящих в состав поставки, отсутствуют сколы, царапины, целостность этикеток и пломб не нарушены;
3. контрольные суммы дистрибутива соответствуют заявленным в Формуляре [4].

### 2.2 Общие сведения

JMS - система, предназначенная для внедрения и учета аппаратных средств аутентификации, защищенных носителей информации (ЗНИ) и средств дистанционной работы (СДР) пользователей в масштабах предприятия.

JMS обеспечивает:

- централизованное управление средствами аутентификации, ЗНИ и СДР в течение всего их жизненного цикла (инициализация/выпуск, ввод в эксплуатацию/выдача, обслуживание, вывод из эксплуатации/блокирование);
- учет средств аутентификации, ЗНИ и СДР; аудит их использования;
- автоматизацию типовых операций и сценариев администрирования в соответствии с политиками безопасности, принятыми в организации;
- быстрое и самостоятельное решение проблем пользователей без обращения к администраторам.

 В настоящем документе описание настроек JMS представлено на примере операционной системы Astra Linux Special Edition (ОС СХ Смоленск 1.6).

### 2.3 Состав JMS

Система JMS развертывается на нескольких компьютерах с ОС Linux и включает в себя следующие компоненты:

- сервер JMS (демон-процесс eap-engine.service) – сервер бизнес-логики JMS;
- консольный агент JMS (процесс Aladdin.EAP.Agent.Terminal) – утилита динамического конфигурирования сервера JMS (всегда устанавливается на том же хосте, что и Сервер JMS);
- серверный компонент web-консоли управления JMS (демон-процесс eap-web-admin.service);
- компонент JMS Web Agent или JWA (процесс jwa-service) – устанавливается на тех компьютерах с ОС Linux, на которых будет выполняться физическое обращение к электронным ключам и защищенным носителям информации (ЗНИ), а именно: на компьютерах с web-приложениями Консоль управления JMS и Клиент JMS.

### 3. Описание пакета установки

Дистрибутив JMS включает следующие пакеты установки.

Табл. 3 – Установочные пакеты сервера JMS

ОС	Файл дистрибутива	Описание
Astra Linux	<b>aladdin-eap-engine_x.x.x.xxxx-x64.deb</b>	Серверная часть JMS (сервер бизнес-логики, консольный агент JMS – утилита динамического конфигурирования сервера JMS)
РЕД ОС	<b>aladdin-eap-engine_x.x.x.xxxx_x64.rpm</b>	
ОС Альт	<b>aladdin-eap-engine_x.x.x.xxxx_alt_x64.rpm</b>	

Табл. 4 – Установочные пакеты серверного web-приложения Консоль управления JMS (JMS Web Admin)

ОС	Файл дистрибутива	Описание
Astra Linux	<b>aladdin-eap-web-admin_x.x.x.xxxx_x64.deb</b>	Серверный компонент, реализующий web-приложение «Консоль управления JMS» (JMS Web Admin)
РЕД ОС	<b>aladdin-eap-web-admin_x.x.x.xxxx_x64.rpm</b>	
ОС Альт	<b>aladdin-eap-web-admin_x.x.x.xxxx_alt_x64.rpm</b>	

Табл. 5 – Установочные пакеты JWA

ОС	Файл дистрибутива	Описание
Astra Linux	<b>aladdin-jms-web-agent_x.x.x.xxx_x64.deb</b>	JMS Web Agent (JWA) -- программное обеспечение работы web-клиента JMS
РЕД ОС, ОС Альт	<b>aladdin-jms-web-agent_x.x.x.xxxx_x64.rpm</b>	

Табл. 6 – Установочные пакеты JWA Tray

ОС	Файл дистрибутива	Описание
Astra Linux	<b>aladdin-jms-web-agent-tray_x.x.x.xxxx_x64.deb</b>	JWA Tray – программное обеспечение графической визуализации статуса web-клиента JMS и простых операций с ЭК
РЕД ОС, ОС Альт	<b>aladdin-jms-web-agent-tray_x.x.x.xxxx_x64.rpm</b>	

## 4. Системные требования

Полный перечень требований к среде функционирования компонентов JMS приведен в Формуляре [4].

### Примечания.


1. Для поддержки работы с СДР ALO требуется наличие библиотеки jcrkcs11 версии 2.8.0.623 (jcrkcs11-2\_2.8.0.623\_al\_x64.deb) или более поздней, подробнее см. раздел «Установка и первоначальная настройка JMS Web Agent (JWA)», с. 24.
2. Для корректного отображения информации в административном web-интерфейсе продукта предьявляется дополнительное требование к минимальному разрешению видеоинтерфейса: 1280 x 720.

## 5. Установка и первоначальная настройка

### 5.1 Начальные условия для развертывания JMS

Для развертывания продукта должны быть выполнены следующие начальные условия.

1. В сетевой доступности для сервера JMS должна быть установлена служба управления учетными записями (ресурсная система). При установке рекомендуется использовать руководство поставщика сервиса <https://wiki.astralinux.ru/display/doc/FreelPA+Astra+Linux>.

 **Примечание.** В настоящем руководстве в качестве примера IP-адреса сервера FreelPA указывается 192.168.10.1; в качестве имени домена FreelPA указывается freeipa.aladdin.local.

2. На компьютерах, на которых предполагается устанавливать сервер JMS, сервер СУБД, JMS-клиенты и консоль управления JMS, должен быть установлен клиентский компонент ресурсной системы (например FreelPA). Все перечисленные типы компьютеров следует зарегистрировать в одном и том же домене ресурсной системы. При установке рекомендуется использовать руководство поставщика сервиса <https://wiki.astralinux.ru/display/doc/FreelPA+Astra+Linux>.
3. В сетевой доступности для сервера JMS должен быть установлен сервер СУБД PostgreSQL версии 9.6.10. При установке могут быть полезны рекомендации поставщика СУБД, см. <https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362076>.
4. На компьютерах, на которых предполагается устанавливать сервер JMS, в зависимости от операционной системы должно быть установлено соответствующее дополнительное ПО поддержки протокола NTLM SSP (Табл. 7).

Табл. 7 – Пакеты дополнительного ПО поддержки NTLM SSP для разных версий ОС Linux

ОС	Имя файла дистрибутива дополнительного ПО
Astra Linux 1.6	gss-ntlmssp_0.7.0-3_amd64
Astra Linux 1.7	gss-ntlmssp_0.7.0-4_amd64
ОС Альт	gssntlmssp-0.7.0-alt1.M80P.2.x86_64
РЕД ОС	gssntlmssp-0.7.0-2.el7.x86_64

Кроме перечисленных выше подготовительных действий, может быть подготовлен сертификат для подсистемы аутентификации JMS (для подписи JWT-токенов) со следующими параметрами:



- сертификат должен быть выпущен для хоста сервера JMS (в сертификате должно быть указано доменное имя данного хоста в ресурсной системе);
- назначение ключа подписи:

```
keyUsage = digitalSignature, keyEncipherment
```

В результате выпуска сертификата должен быть получен файл контейнера сертификата с закрытым ключом (файл .pfx).

Сертификат должен быть зарегистрирован средствами ОС на хосте с сервером JMS в хранилище *CurrentUser\My*.



**Примечание.** В настоящем руководстве в качестве примера JWT-сертификата используется самоподписанный сертификат.

В случае если сертификат для подсистемы аутентификации JMS не установлен, то используется подпись JWT-токенов внутренними ключами сервера JMS (подробнее см. использование команды `Aladdin.EAP.Agent.Terminal jwt configure --useCertificate false`, раздел «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83)

## 5.2 Установка и первоначальная настройка сервера и консольного агента JMS



**Примечание.** Все команды в данном разделе выполняются в контексте пользователя `root`.

### 5.2.1 Подготовительные действия

Для подготовки к развертыванию сервера JMS и консольного агента JMS выполните следующие действия.

1. Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки JMS, следующие файлы:
  - Установочный пакет сервера JMS согласно Табл. 3, с. 15.
  - `InitialConfiguration.ini`
2. В предварительно созданную папку (в текущем документе в качестве примера используется папка `/opt/licenses`) скопируйте файл лицензии (с расширением `.lic`), полученный у поставщика продукта.
3. В папке с `deb`-файлом сервера создайте файл первоначальной конфигурации сервера JMS `InitialConfiguration.ini` по следующему образцу:

```
[service]
execPath=/opt/eap-engine/Aladdin.EAP.Engine
integrationManagerUrls=http://*:8120
controlManagerUrls=http://localhost:8119
authenticationManagerUrls=http://*:8121
clientManagerUrls=http://*:8122

[database]
type=PostgreSQL
serverAddress=localhost
serverPort=5432
databaseName=JMS4DB_2021_09_17
serverLogin=postgres
serverPassword=P@ssw0rd
databaseLogin=postgres
databasePassword=P@ssw0rd

[accountSystem]
```

```
type=FreeIPA
name=DirectoryAlias
serverAddress=172.16.12.42
serverPort=389
container=dc=astratest,dc=local
userName=uid=admin,cn=users,cn=accounts,dc=astratest,dc=local
password=P@ssw0rd

[primaryUser]
accountName=admin

[licenses]
path=/opt/licenses/EAP.lic

[sts]
certificateThumbprint=4CEFFDE06B759319EA9946D78BEB28A25C3DB14D
```

В параметре *path* из секции *[licenses]* укажите имя файла лицензии вместе с полным путем к нему, созданного на шаге 2.

Назначение остальных параметров файла конфигурации приведено в разделе «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78.



**Примечание.** В случае если обращение к ресурсной системе требует осуществлять по протоколу SSL, в секции *[AccountSystem]* следует также добавить параметр *useSsl=true* и убедиться в корректности значения параметра *serverPort* (636 для SSL, значение по умолчанию). Подробнее см. в разделах «Настройка SSL для доступа к ресурсной системе», с. 63 и «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78.

4. На хосте с установленной СУБД PostgreSQL следует установить дополнительный компонент с помощью следующей команды:

```
apt install postgresql-contrib
```

## 5.2.2 Установка компонентов сервера JMS

1. Установите на текущем хосте сервер JMS с помощью соответствующей команды.

- 1.1. Для ОС Astra Linux:

```
dpkg -i <путь_к_файлу_deb-пакета_согласно_Табл. 3, с. 15>
```

- 1.2. Для РЕД ОС:

```
sudo dnf install <путь_к_файлу_rpm-пакета_согласно_Табл. 3, с. 15>
```

- 1.3. Для ОС Альт:

```
sudo apt-get install <путь_к_файлу_rpm-пакета_согласно_Табл. 3, с. 15>
```

По окончании успешной установки должна отобразиться информация следующего вида:

```


dpkg: предупреждение: анализ файла «/var/lib/dpkg/tmp.ci/control» около строки 9 пакета «eap-engine»:
отсутствует description
dpkg: предупреждение: анализ файла «/var/lib/dpkg/tmp.ci/control» около строки 9 пакета «eap-engine»:
отсутствует maintainer
Выбор ранее не выбранного пакета eap-engine.
(Чтение базы данных ... на данный момент установлено 149393 файла и каталогов.)
Подготовка к распаковке ./eap-engine_4.0.0.5100.deb ...
Распаковывается eap-engine (4.0.0.5100) ...
Настраивается пакет eap-engine (4.0.0.5100) ...
[Unit]
Description=EAP Engine Service
DefaultDependencies=no
[Service]
Type=simple
RemainAfterExit=no
ExecStart=/usr/bin/sudo /opt/eap-engine/Aladdin.EAP.Engine
WorkingDirectory=/opt/eap-engine
User=root
Group=root
[Install]
WantedBy=multi-user.target
Created symlink /etc/systemd/system/multi-user.target.wants/eap-engine.service → /etc/systemd/system/eap-engine.service.

```

Рис. 1 – Информация в консоли в случае успешной установки сервера JMS

2. Выполните начальное конфигурирование сервера JMS с помощью следующей команды консольного агента:

```
sudo Aladdin.EAP.Agent.Terminal server initialize -p
/var/jms4/conf/InitialConfiguration.ini
```

 **Примечание.** Полное описание команд консольного агента см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83.

По окончании конфигурирования в консоли должна отобразиться строка «Инициализация сервера завершена успешно».

```

Чтение лицензий из директории /opt/licenses...
/opt/eap-engine/HostConfig.xml
Конфигурация базы данных...
База данных JMS4DB создана успешно.
Остановка EAP-сервиса...
Конфигурация EAP-сервиса...
Запуск EAP-сервиса...
EAP-сервис запущен.
Запуск мастера-настройки...
Инициализация сервера завершена успешно.
root@jmsserver:/opt/licenses# █

```

Рис. 2 – Сообщение в консоли об успешной начальной настройке сервера JMS

3. Проверьте статус службы сервера JMS следующей командой.

```
systemctl status eap-engine
```

Состояние должно быть «active (running)»:

```

root@jmsserver:/opt/licenses# systemctl status eap-engine
● eap-engine.service - EAP Engine Service
   Loaded: loaded (/etc/systemd/system/eap-engine.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-04-01 12:46:42 MSK; 40s ago
     Main PID: 14782 (sudo)
       Tasks: 33 (limit: 4915)
    CGroup: /system.slice/eap-engine.service
            └─14782 /usr/bin/sudo /opt/eap-engine/Aladdin.EAP.Engine
              └─14784 /opt/eap-engine/Aladdin.EAP.Engine

apr 01 12:46:53 jmsserver.aladdin.local Aladdin.EAP.Engine[14784]: ConfigurationManager: Изм

```

Рис. 3 – Отображение статуса службы сервера JMS

4. Проверьте статус сервера бизнес-логики JMS с помощью следующей команды консольного агента

```
Aladdin.EAP.Agent.Terminal server status
```

В случае корректной работы сервера бизнес-логики должна отобразиться строка «Текущее состояние сервера: Работает».

### 5.3 Установка и первоначальная настройка серверного web-приложения Консоль управления JMS (JMS Web Admin)

#### 5.3.1 Подготовительные действия

Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки серверного Web-приложения, дистрибутивный файл Консоли управления согласно Табл. 4, с. 15.

#### 5.3.2 Установка серверного компонента Консоли управления JMS



**Примечание.** Все команды в данном разделе выполняются в контексте пользователя root.

1. Установите серверный компонент web-приложения Консоль управления JMS с помощью соответствующей команды.

- 1.1. Для ОС Astra Linux:

```
dpkg -i <путь_к_файлу_deb-пакета_согласно_Табл. 4, с. 15>
```

- 1.2. Для РЕД ОС:

```
sudo dnf install <путь_к_файлу_rpm_пакета_согласно_Табл. 4, с. 15>
```

- 1.3. Для ОС Альт:

```
sudo apt-get install <путь_к_файлу_rpm_пакета_согласно_Табл. 4, с. 15>
```

По окончании успешной установки должна отобразиться информация следующего вида:

```
Настраивается пакет eap-admin-web (4.0.0.30) ...
[Unit]
Description=EAP WebAdmin Service
DefaultDependencies=no
[Service]
Type=simple
RemainAfterExit=no
Restart=always
RestartSec=10
ExecStart=/opt/eap-admin-web/Aladdin.EAP.Admin.Web
WorkingDirectory=/opt/eap-admin-web
User=root
Group=root
[Install]
WantedBy=multi-user.target
Created symlink /etc/systemd/system/multi-user.target.wants/eap-web-admin.service → /etc/sy
```

Рис. 4 – Информация в консоли в случае успешной установки серверного web-приложение Консоль управления JMS

- В папке `/opt/eap-web-admin/` отредактируйте файл `appsettings.json`. Исходная версия данного файла конфигурации выглядит следующим образом:

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "AllowedHosts": "*",

  "IntegrationApiUrl": "http://localhost:8120",
  "AuthenticationApiUrl": "http://localhost:8121",

  "Kestrel": {
    "Endpoints": {
      "Http": {
        "Url": "http://0.0.0.0:5000"
      }
    }
  }
}
```

В случае если серверный компонент консоли управления JMS установлен на хосте, отличном от хоста с сервером JMS, то в полях *IntegrationApiUrl* и *AuthenticationApiUrl* следует указать адрес хоста с сервером JMS (номера портов следует сохранить прежними).

Настройку адреса в параметре *Url* следует выполнять следующим образом:

- если необходимо обеспечить обработку запросов, поступающих только на IPv4-интерфейсы хоста, то в адресе следует указать `http://0.0.0.0:5000` (значение по умолчанию);
- если необходимо обеспечить обработку запросов, поступающих только на IPv6-интерфейсы хоста, то в адресе следует указать `http://[::]:5000`;
- если необходимо обеспечить обработку запросов, поступающих на все IPv4- и IPv6-интерфейсы хоста, то в адресе следует указать `http://*:5000`;
- если необходимо обеспечить обработку запросов, поступающих только с локального хоста, то в адресе следует указать `http://localhost:5000` либо `http://127.0.0.1:5000` (`http://[::1]:5000` для IPv6);
- если необходимо обеспечить обработку запросов, поступающих на конкретный интерфейс хоста, то в адресе следует указать адрес данного сетевого интерфейса, например `http://192.168.1.100:5000`;
- порядок настройки SSL для серверного web-приложения Консоль управления JMS приведен в разделе «Настройка SSL/TLS на стороне Web-приложения Консоль управления JMS», с. 59.

При необходимости ограничить поступления запросов из внешней сети по IP-адресам используйте встроенные сетевые средства операционной системы или внешний межсетевой экран.

- Перезапустите службу серверного компонента консоли управления JMS, выполнив следующую команду:

```
systemctl restart eap-web-admin
```

4. Проверьте статус службы.

```
systemctl status eap-web-admin
```

Состояние должно быть «active (running)»:

```
● eap-web-admin.service - EAP WebAdmin Service
   Loaded: loaded (/etc/systemd/system/eap-web-admin.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-04-01 12:51:40 MSK; 8s ago
     Main PID: 15105 (Aladdin.EAP.Adm)
        Tasks: 18 (limit: 4915)
      CGroup: /system.slice/eap-web-admin.service
              └─15105 /opt/eap-admin-web/Aladdin.EAP.Admin.Web

анр 01 12:51:40 jmsserver.aladdin.local systemd[1]: Stopped EAP WebAdmin Service.
анр 01 12:51:40 jmsserver.aladdin.local systemd[1]: Started EAP WebAdmin Service.
анр 01 12:51:41 jmsserver.aladdin.local Aladdin.EAP.Admin.Web[15105]: info: Microsoft.Hosting.L
```

Рис. 5 – Отображение статуса службы серверного компонента консоли управления JMS

5. Для проверки корректности установки web-приложения Консоль управления JMS на хосте с сервером JMS запустите веб-браузер Firefox и введите в нем адрес, установленный на шаге 2 в конфигурационном файле `appsettings.json` для атрибута `Url` (по умолчанию <http://localhost:5000>). Отобразится страница следующего вида.

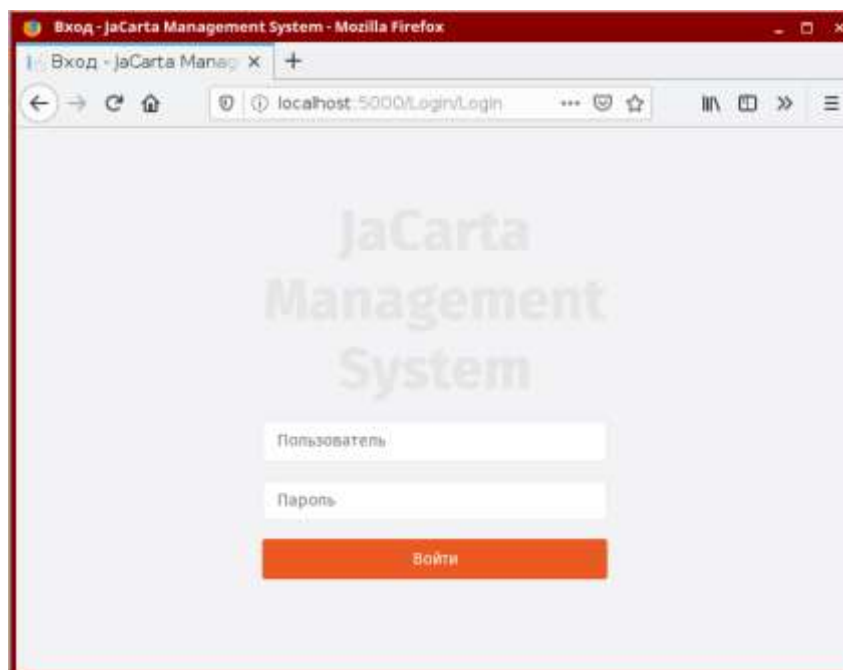



Рис. 6 – Стартовая страница Web-приложения Консоль управления JMS

### 5.3.3 Проверка работы web-приложения Консоль управления JMS

1. С внешней машины в web-браузере выполните подключение к web-консоли JMS по адресу

```
http://<IP-адрес_сервера_web-консоли>:5000
```

где <IP-адрес\_сервера\_web-консоли> – IP-адрес или FQDN-имя компьютера с установленным серверным web-приложением Консоль управления JMS.

 **Примечание.** В случае настройки защищенного соединения по SSL/TLS в адресе укажите `https://`.  
Отобразится страница следующего вида.

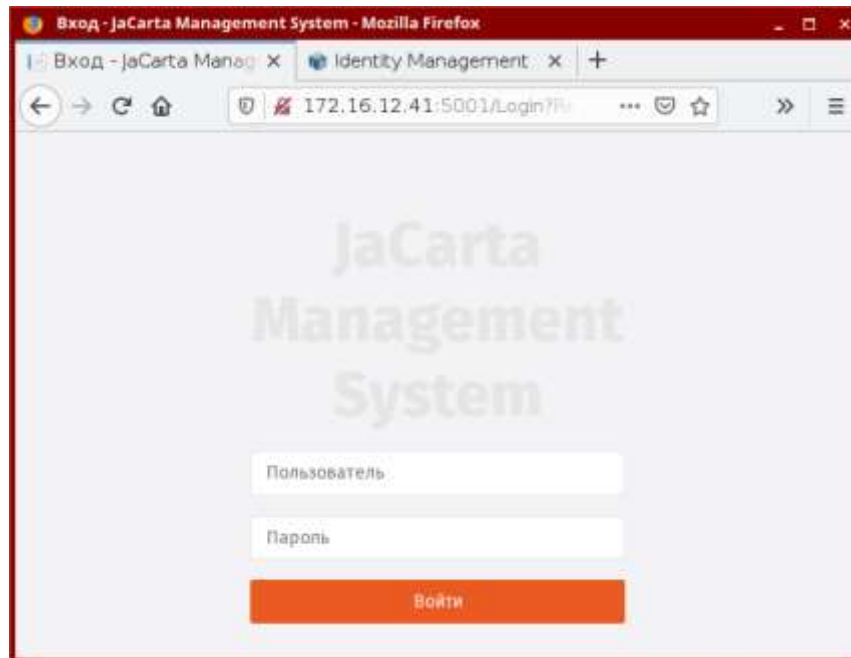


Рис. 7 – Доступ к web-консоли JMS с внешнего компьютера

2. В поле **Пользователь** введите логин пользователя в формате:  
<имя\_ресурсной\_системы>\<имя\_пользователя>,  
где <имя\_ресурсной\_системы> – значение, указанное в поле [accountSystem] -> name  
файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной  
конфигурации сервера JMS», с. 78).  
Например:

DirectoryAlias\admin

 **Примечание.**

Альтернативным способом аутентификации пользователя является указание в качестве доменного префикса:

- для **AD** и **SambaAD**: netbios-имени домена. Например для домена aladdin.local и пользователя admin допускается ввести значение aladdin\admin
- для **FreeIPA**: полного или FQDN-имени домена. Например для домена astratest.local и пользователя admin допускается ввести значение astratest.local\admin

После ввода аутентификационных данных отобразится страница следующего вида.

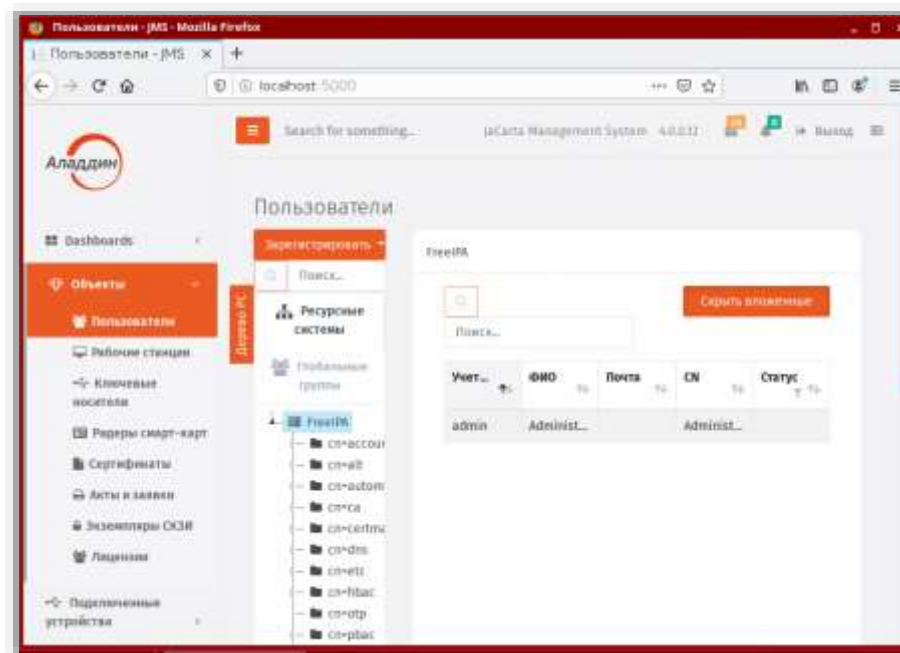


Рис. 8 – Стартовая страница web-приложения Консоль управления JMS

Web-приложение Консоль управления JMS готово к работе.

#### 5.3.4 Дополнительные настройки

Для начала работы в JMS может понадобиться добавить поддержку дополнительных типов токенов (электронных ключей, ЭК).

Порядок добавления токенов описан в разделе «Добавление поддержки моделей ЭК / профилей в JMS», с. 48.

### 5.4 Установка и первоначальная настройка JMS Web Agent (JWA)

Компонент JWA следует устанавливать на компьютерах, предназначенных для работы из клиентских web-приложений (Клиент JMS и Консоль управления JMS).



**Примечание.** Все команды в данном разделе выполняются в контексте пользователя root.

#### 5.4.1 Подготовительные действия

Для подготовки к развертыванию компонента JMS Web Agent (JWA) выполните следующие действия.

1. Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки JWA, следующие файлы:
  - jcrkcs11-2\_x.x.x.xxx\_al1.6\_x64.deb – единая библиотека JaCarta;
  - дистрибутив JWA согласно Табл. 5, с. 15.
2. Для корректной работы Единой библиотеки JaCarta установите фоновую службу PC/SC следующей командой:



```
apt install pcscd
```

- Установите единую библиотеку JaCarta следующей командой:

```
dpkg -i jcpkcs11-2_x.x.x.xxx_al1.6_x64.deb
```

При успешной установке должна отобразиться информация следующего вида:

```
Распаковывается jcpkcs11-2 (2.7.0.461) ...
Настраивается пакет jcpkcs11-2 (2.7.0.461) ...
searching for Info.plist to update...
checking /etc/libccid_Info.plist
updating /etc/libccid_Info.plist
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
update_ifd_ccid_bundle.sh [user.warning] No need to update any section
checking updated /etc/libccid_Info.plist
pcscd version 1.8.24.
[ ok ] Restarting pcscd (via systemctl): pcscd.service.
```

Рис. 9 – Индикация успешной установки единой библиотеки JaCarta



**Примечание.** В случае обновления ПО JMS, при условии, что обновляется также единая библиотека JaCarta перед установкой нового пакета с единой библиотекой следует удалить ранее установленную. Для удаления устаревшей единой библиотеки JaCarta используйте команду:

```
sudo dpkg -r jcpkcs11-2
```

#### 5.4.2 Установка JWA

- Установите компонент JMS Web Agent (JWA), выполнив соответствующую команду.

- Для ОС Astra Linux:

```
dpkg -i <путь_к_файлу_deb-пакета_согласно_Табл. 5, с. 15>
```

- Для РЕД ОС:

```
dnf install <путь_к_файлу_gpm-пакета_согласно_Табл. 5, с. 15>
```

- Для ОС Альт:

```
apt-get install <путь_к_файлу_gpm-пакета_согласно_Табл. 5, с. 15>
```

По окончании успешной установки должна отобразиться информация следующего вида:

```
execstart=/usr/bin/sudo /opt/jms-client/Aladdin.JMS.WebAgent
WorkingDirectory=/opt/jms-client
User=root
Group=root
[Install]
WantedBy=multi-user.target
Set Aladdin JMS Web Agent to start at boot ...
Running jwa-service ...
Created symlink /etc/systemd/system/multi-user.target.wants/jwa-service.service → /etc/sys
```

Рис. 10 – Индикация успешной установки компонент JMS Web Agent

- Выполните остановку процесса JWA командой:

```
/opt/jms-client/jwa-service.sh stop
```

3. Выполните конфигурирование компонента JWA на текущем хосте с помощью команды следующего вида

```
<путь>/Aladdin.JMS.WebAgent --jms-host <Сервер_JMS> --jms-web-host  
<Сервер_JMS_Web_Admin>
```

где <путь> – путь к исполняемому файлу JWA;  
<Сервер\_JMS> – FQDN-имя сервера JMS;  
<Сервер\_JMS\_Web\_Admin> – FQDN-имя сервера с серверным компонентом web-приложения «Консоль управления JMS».

Например:

```
/opt/jms-client/Aladdin.JMS.WebAgent --jms-host jmsserver.aladdin.local --jms-web-host jmsserver.aladdin.local
```

По окончании успешного конфигурирования в консоли должна отобразиться строка «Configuration appsettings.json is updated».



**Примечание.** Полный перечень команд JWA см. в разделе «Приложение 5. Справочник команд JMS Web Agent (JWA)», с. 106.

4. Запустите процесс JWA командой:

```
/opt/jms-client/jwa-service.sh bg
```

5. Для проверки корректности работы процесса JWA на данном хосте запустите веб-браузер Firefox и перейдите в нем по адресу <https://localhost:5600>. Должна отобразиться страница следующего вида.

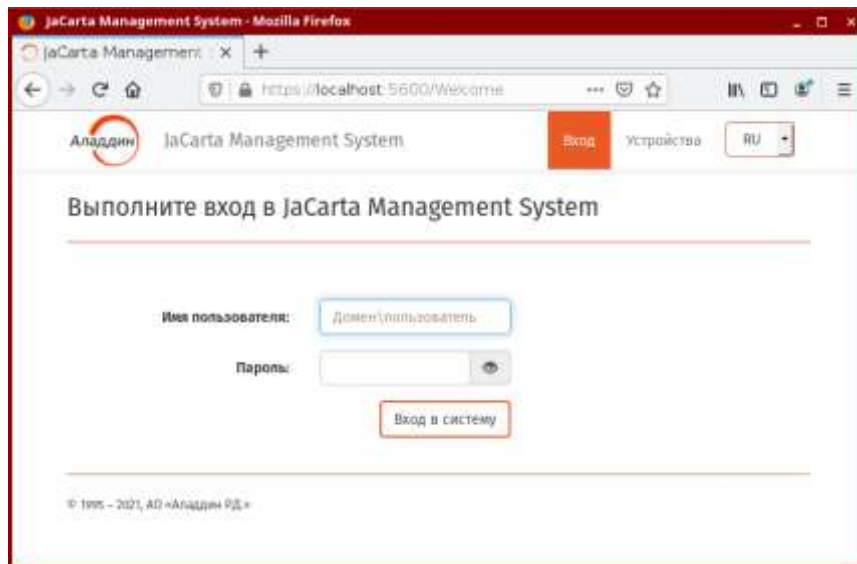


Рис. 11 – Стартовая страница web-приложения Клиент JMS



**Примечания:**

1. При необходимости дополнительные настройки компонента JWA можно выполнить путем редактирования файла /etc/aladdin/jwa-service/appsettings.json.
2. После внесения изменений файл конфигурации appsettings.json для вступления в силу новых параметров следует перезапустить процесс JWA (см. раздел «Управление процессом JWA», с. 27).
3. Для автоматической аутентификации пользователя по протоколу Kerberos необходимо выполнить дополнительные настройки, описанные в разделе «Порядок настройки прозрачной аутентификации доменных пользователей AD в клиентских приложениях JMS», с. 66.

### 5.4.3 Управление процессом JWA

Для управления процессом JWA используется файл сценария `/opt/jms-client/jwa-service.sh` (развертывается автоматически вместе с компонентом JWA).

Для запуска процесса JWA в фоновом режиме используется команда:

```
/opt/jms-client/jwa-service.sh bg
```

Для остановки процесса JWA используется команда:

```
/opt/jms-client/jwa-service.sh stop
```

Для перезапуска процесса используйте команды:

```
/opt/jms-client/jwa-service.sh stop  
/opt/jms-client/jwa-service.sh bg
```



**Примечание.** В отладочных целях может также использоваться команда

```
/opt/jms-client/jwa-service.sh start
```

Она позволяет мониторить записи журнала процесса JWA, которые отображаются в интерактивном режиме в терминале. При закрытии терминала процесс JWA в этом случае автоматически останавливается.

### 5.4.4 Проверка работы JWA с Консолью управления JMS

Для того чтобы проверить корректность работы установленной службы JWA (см. разделы 5.4.1 и 5.4.2, выше) совместно с web-приложением Консоль управления JMS, запустите веб-браузер Firefox и перейдите в нем по адресу, указанному в параметре `--jms-web-host` (т.е. адреса серверного компонента web-приложения Консоль управления JMS) команды конфигурирования JWA (см. п. 3 раздела «Установка JWA», с. 26).

Отобразится страница следующего вида.

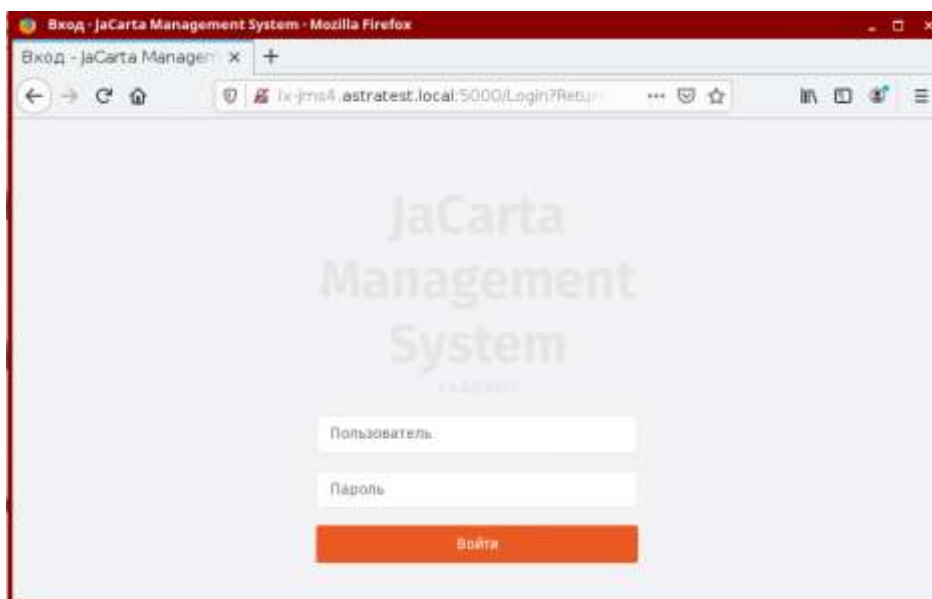


Рис. 12 – Страница аутентификации в Web-приложении Консоль управления JMS

Выполните аутентификацию так, как это описано в разделе «Проверка работы web-приложения Консоль управления JMS», с. 22.

Отобразится страница следующего вида.

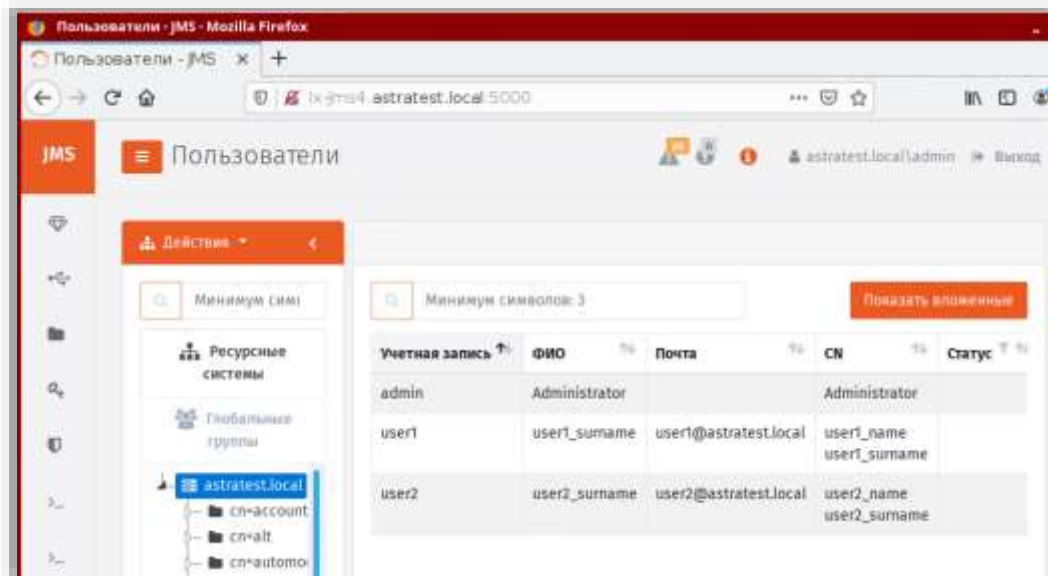


Рис. 13 – Вид страницы Консоли управления с корректно подключенным компонентом JWA

В случае если вверху страницы отображается индикация ошибки соединения с JWA (Рис. 14), следует проверить корректность настроенных адресов серверного компонента Консоли управления в секции CORS файла конфигурации файла `/etc/aladdin/jwa-service/appsettings.json` и при необходимости повторно выполнить команду конфигурирования JWA (см. «Приложение 5. Справочник команд JMS Web Agent (JWA)», с. 106).

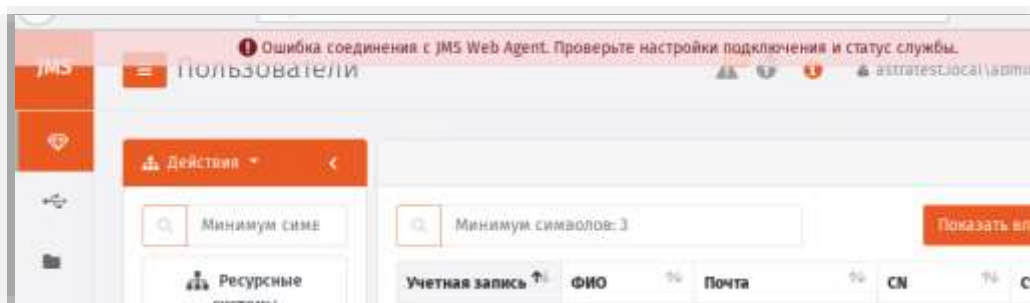


Рис. 14 – Ошибка подключения к компоненту JWA из клиентского web-приложения Консоль управления JMS

## 5.5 Установка и первоначальная настройка приложения JMS Web Agent Tray

Компонент JMS Web Agent Tray следует устанавливать на компьютерах конечных пользователей, использующих ЭК/ЗНИ/СДР.

Компонент позволяет выполнять аутентификацию пользователя JMS для того, чтобы выполнять монтирование скрытых разделов ЗНИ, в фоновом режиме осуществлять синхронизацию электронных ключей, подключенных к компьютеру. Кроме того, компонент упрощает процедуру запуска web-клиента JMS.



**Примечание.** Все команды в данном разделе выполняются в контексте пользователя root.

### 5.5.1 Подготовительные действия

Для подготовки к развертыванию компонента JMS Web Agent Tray выполните следующие действия.

1. Убедитесь, что на компьютере установлен компонент JWA (см. раздел «Установка и первоначальная настройка JMS Web Agent (JWA)», с. 24)
2. Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки компонента, дистрибутив JWA Tray согласно Табл. 6, с. 15.

### 5.5.2 Установка JWA Tray

1. Установите компонент JWA Tray, выполнив соответствующую команду.

- 1.1. Для ОС Astra Linux:

```
dpkg -i <путь_к_файлу_deb-пакета_согласно_Табл._6,_с._15>
```

- 1.2. Для РЕД ОС:

```
dnf install <путь_к_файлу_rpm-пакета_согласно_Табл._6,_с._15>
```

- 1.3. Для ОС Альт:

```
apt-get install <путь_к_файлу_rpm-пакета_согласно_Табл._6,_с._15>
```

По окончании успешной установки должна отобразиться информация следующего вида:

```
dpkg: предупреждение: анализ файла «/var/lib/dpkg/status» около строки 32734 пакета «offline-ca-adapter»:
отсутствует maintainer
Выбор ранее не выбранного пакета aladdin.jms.webagenttray.
(Чтение базы данных ... на данный момент установлено 160752 файла и каталога.)
Подготовка к распаковке .../aladdin-jms-web-agent-tray_4.0.0.5300_x64.deb ...
Распаковывается aladdin.jms.webagenttray (4.0.0.5300.linux-x64) ...
Настраивается пакет aladdin.jms.webagenttray (4.0.0.5300.linux-x64) ...
root@lx-jms4:/var/jms4/distr#
```

Рис. 15 – Индикация успешной установки компонент JWA Tray

1. После установки компонента в области уведомлений рабочего стола операционной системы появится значок **W**, при нажатии на котором правой кнопкой мыши отобразится меню следующего вида.

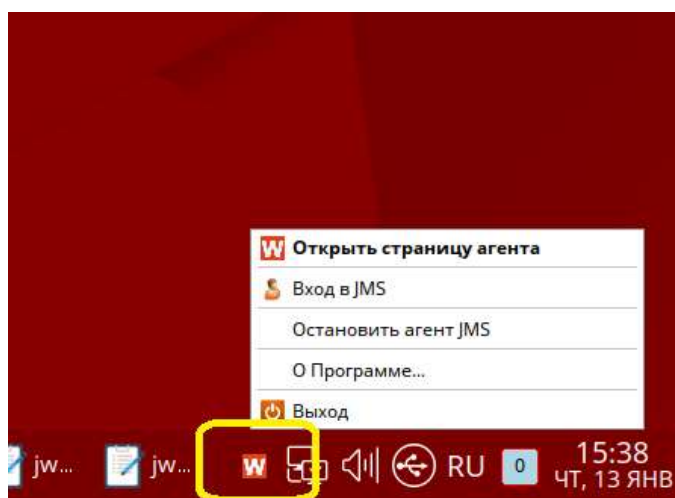



Рис. 16 – Отображение значка JWA Tray и соответствующего контекстного меню

Начальное меню JWA Tray содержит следующие пункты (Табл. 8).

Табл. 8 – Описание начального меню JWA Tray

Пункт меню	Описание
Открыть страницу агента	Открытие в web-браузере сеанса работы web-клиента JMS с сервером JMS, адрес которого установлен в настройках JWA.  Сеанс запускается в том web-браузере, который установлен в данной операционной системе по умолчанию.
Вход в JMS	Открытие окна ввода аутентификационных данных пользователя JMS для его аутентификации на сервере JMS для дальнейшей работы с подключаемыми ЭК/ЗНИ/СДР в фоновом режиме (без необходимости запуска web-клиента JMS)   <b>Примечание.</b> Для автоматической аутентификации пользователя по протоколу Kerberos необходимо выполнить дополнительные настройки, описанные в разделе «Порядок настройки прозрачной аутентификации доменных пользователей AD в клиентских приложениях JMS», с. 66.
Остановить агент JMS / Запустить агент JMS	Остановка процесс jwa-service, например, для выполнения его «ручного» конфигурирования
О программе	Получение информации о программе
Выход	Прекращение работы программы JWA Tray (процесс WebAgentTray)



**Примечание.** Компонент JWA Tray (процесс WebAgentTray) считывает конфигурацию из файла jwa.systray.settings.ini.

## 5.6 Обеспечение поддержки СДР ALO на клиентских компьютерах

Для обеспечения в JMS поддержки USB-носителей СДР ALO на клиентских компьютерах, на которых предполагается использовать данные носители, в директорию `/usr/lib` следует скопировать следующие файлы:

- flash2.dll
- libflash2.so

из комплекта поставки «Средства обеспечения безопасной дистанционной работы Aladdin LiveOffice» (подробнее см. документацию СДР ALO [6], список литературы на с. 114)

Кроме того, для поддержки работы с СДР ALO на клиентских компьютерах требуется наличие установленной библиотеки jcrkcs11 версии 2.8.0.623 (jcrkcs11-2\_2.8.0.623\_al\_x64.deb) или более поздней, подробнее см. раздел «Установка и первоначальная настройка JMS Web Agent (JWA)», с. 24.

## 6. Активация продукта

Изначально продукт поставляется с «активационной» лицензией. После установки такой лицензии работа продукта в полнофункциональном режиме возможна лишь на протяжении «активационного» периода, определённого в такой лицензии (обычно 2 недели, Рис. 17).

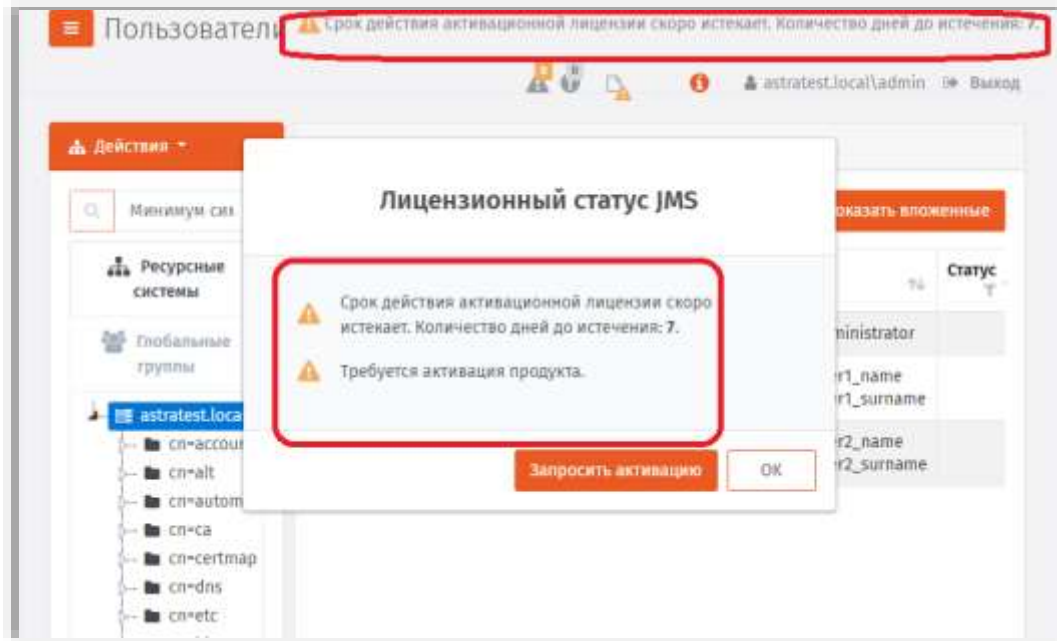


Рис. 17 – Отображение признаков активационной лицензии в консоли управления JMS

По окончании активационного периода все основные функции продукта (кроме возможности замены/установки лицензии) блокируются до момента установки постоянной лицензии, Рис. 18.

**Примечание.** Активационный период обеспечивает функционирование продукта в тестовом режиме и не входит в фактически оплаченный период действия пользовательской лицензии на продукт.

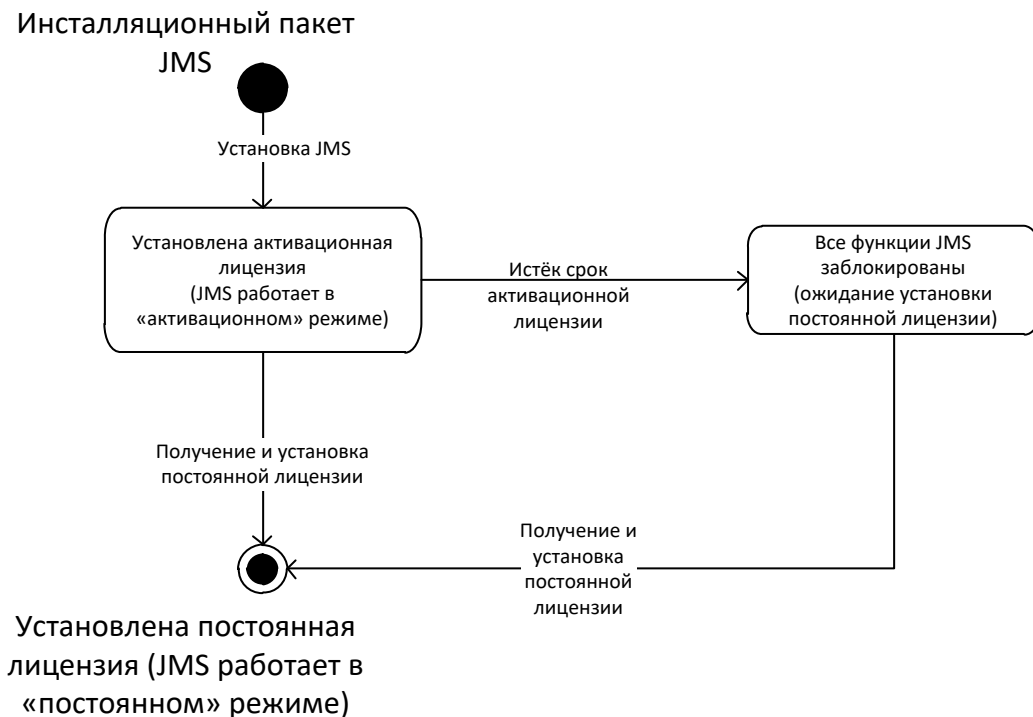


Рис. 18 – Диаграмма переходов для процедуры активации JMS

Для перевода продукта в режим обычной работы («постоянный» режим), следует установить постоянную лицензию (выдается производителем пользователю JMS после создания им файла «Запрос на активацию», который генерируется в интерактивном режиме из консоли управления JMS).

Для формирования запроса на получение постоянной лицензии в окне лицензионного статуса (Рис. 19) следует нажать **Запросить активацию**.

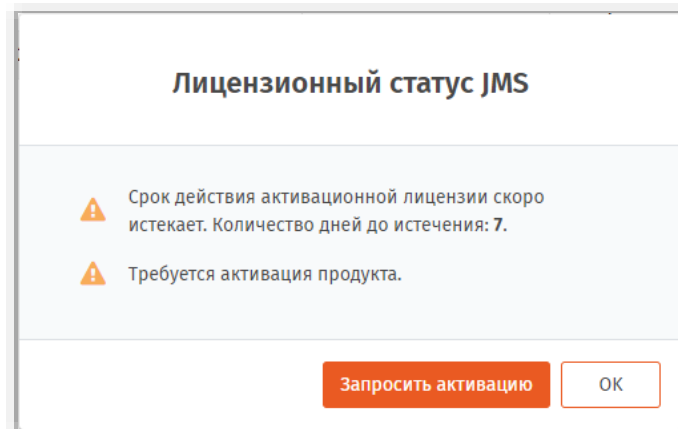


Рис. 19 – Окно лицензионного статуса в Консоли управления JMS

При этом отобразится окно следующего вида (Рис. 20).

Рис. 20 – Форма запроса учетных данных пользователя JMS

#### **Примечания:**

1. Окно запроса лицензионного статуса можно вызвать в любой момент времени, нажав значок лицензии в верхнем правом углу страницы Консоли управления JMS (Рис. 21).
2. Запрос на активацию можно сформировать также с помощью команды `licenses replace` консольного агента; подробное описание формата команды см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 37.



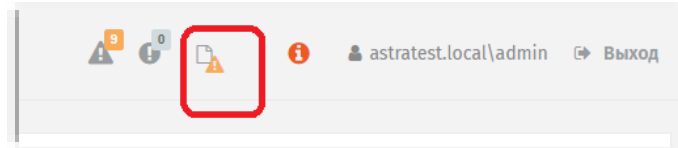


Рис. 21 – Значок для вызова запроса на активацию в неактивированной версии JMS

Заполните поля формы создания запроса на активацию, отметьте флаг согласия с условиями использования продукта и обработки данных и нажмите **Сохранить**. PDF-файл (*JMS\_Activation\_request.pdf*) с запросом на постоянную лицензию будет автоматически сохранен в папку загрузок web-браузера.

Полученный файл следует отправить по адресу [JmsLic@aladdin.ru](mailto:JmsLic@aladdin.ru).

После получения ответа с файлом постоянной лицензии, его следует установить в JMS с помощью команды *licenses replace* консольного агента, например:

```
Aladdin.EAP.Agent.Terminal licenses replace -p /var/jms4/distr/Test_Production_Full.lic
```

На запрос команды имени имя пользователя введите логин пользователя с ролью *Оператор* (в случае начальной установки допускается введение имени пользователя с ролью *Администратор ИБ*) в формате:

```
<имя_ресурсной_системы>\<имя_пользователя>,  
где <имя_ресурсной_системы> – значение, указанное в поле [accountSystem] -> name  
файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной  
конфигурации сервера JMS», с. 78); и пароль данного пользователя:
```

```
root@lx-jms4:/var/jms4/distr# Aladdin.EAP.Agent.Terminal licenses replace -p /var/jms4/distr/Test_Production_Full.lic  
Введите имя пользователя:  
astratest.local\admin  
Введите пароль:  
Лицензия 3 по пути /var/jms4/distr/Test_Production_Full.lic успешно зарегистрирована.
```

Рис. 22 – Консольный диалог при замене лицензии

Подробное описание формата команды см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83

Вступившие в силу параметры новой лицензии можно посмотреть в консоли управления JMS в разделе **Настройки -> Лицензия** (Рис. 23).

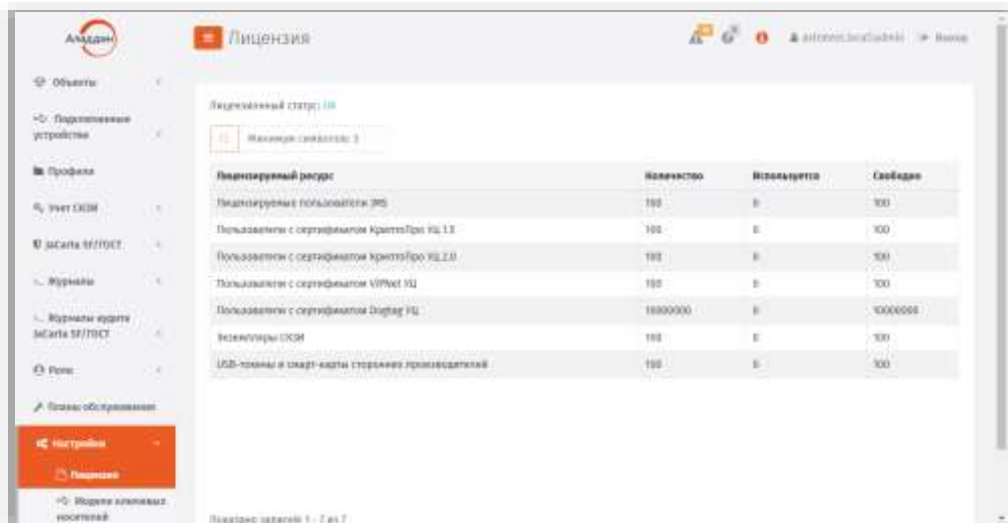


Рис. 23 – Отображение параметров лицензии

## 7. Порядок обновления компонентов JMS

Обновление JMS осуществляется в следующем порядке:

1. «Остановка служб компонентов JMS», с. 34;
2. «Резервное копирование БД JMS», с. 35;
3. «Удаление компонентов JMS», с. 35;
4. «Установка новой версии сервера JMS (в рамках обновления продукта)», с. 35;
5. «Обновление БД JMS», с. 35;
6. «Установка остальных компонентов JMS (в рамках обновления продукта)», с. 35;
7. «Запуск и проверка работоспособности компонентов JMS», с. 36.

### 7.1 Остановка служб компонентов JMS

Выполните остановку служб компонентов следующими командами.

1. Для остановки серверного компонента web-приложения Консоль управления JMS выполните команду:

```
systemctl stop eap-web-admin
```

2. Для остановки службы сервера JMS выполните команду:


```
systemctl stop eap-engine
```

3. Для остановки процесса JWA выполните команду:

```
/opt/jms-client/jwa-service.sh stop
```

4. В случае если в системе развернут также сервер JAS, его также следует остановить. Для остановки компонента JAS выполните команду:

```
systemctl stop jas-engine
```

 **Примечание.** Подробнее см. в руководстве по установке и настройке JAS [3].

## 7.2 Резервное копирование БД JMS

Выполните резервное копирование БД JMS средствами СУБД (PostgreSQL).

## 7.3 Удаление компонентов JMS

Для удаления компонентов JMS выполните следующие команды.

1. Для удаления серверного компонента web-приложения Консоль управления JMS выполните команду:

```
apt remove eap-web-admin
```

2. Для удаления сервера JMS и консольного агента выполните команду:

```
apt remove eap-engine
```

3. Для удаления приложения JMS Web Agent Tray (если устанавливалось) выполните команду:

```
apt remove aladdin.jms.webagenttray
```

4. Для удаления службы компонента JWA выполните команду:

```
apt remove aladdin.jms.webagent
```

5. В случае если в системе также развернут сервер JAS, удалите его согласно руководству по установке и настройке JAS [3].

## 7.4 Установка новой версии сервера JMS (в рамках обновления продукта)

Установите новую версию компонента `aladdin-eap-engine_x.x.x.xxxx.deb` (при обновлении сервера не потребуется повторно создавать и настраивать файл первоначальной конфигурации `InitialConfiguration.ini`: системный конфигурационный файл сервера JMS при обновлении продукта берется в качестве исходного при конфигурировании новой версии продукта).

## 7.5 Обновление БД JMS

Для обновления БД JMS выполните следующую команду консольного агента:

```
sudo Aladdin.EAP.Agent.Terminal server update
```

### Примечания:

1. При выполнении обновления БД могут быть запрошены аутентификационные данные, используемые для запроса статуса службы сервера JMS (запущена / не запущена). В качестве таких данных может использоваться любая учетная запись пользователя, зарегистрированного в JMS и незаблокированного в JMS и в соответствующей ресурсной системе (FreeIPA, AD, SambaAD). В частности, допускается указать аутентификационные данные пользователя, зарегистрированные в параметре «`userName`» в секции [accountSystem] файла первоначальной конфигурации с указанием домена в формате, приведенном в описании параметра «`name`» того же файла (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78).
2. Подробнее с командой `Aladdin.EAP.Agent.Terminal server update` можно ознакомиться в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83.

## 7.6 Установка остальных компонентов JMS (в рамках обновления продукта)

Для установки остальных компонентов новой версии JMS выполните следующие действия.

1. Установите новую версию серверного компонента web-приложения Консоль управления JMS (по аналогии с разделом «Установка серверного компонента Консоли управления JMS», с. 20).
2. В случае если в системе также используется сервер JAS, выполните его обновление согласно руководству по установке и настройке JAS [3].

3. Установите компонент JWA на всех хостах с клиентскими web-приложениями JMS (Клиент JMS и Консоль управления JMS), руководствуясь разделом «Установка JWA», с. 25.

## 7.7 Запуск и проверка работоспособности компонентов JMS

Выполните запуск и проверку работы компонентов JMS в соответствии описаниями в разделе «Установка и первоначальная настройка», с. 16.


## 8. Журналы диагностики JMS

Файлы журналов диагностики JMS записываются по умолчанию в каталог `/var/log/aladdin`, в частности в каталоги:

- `/var/log/aladdin/ear-engine` – журнал диагностики сервера JMS;
- `/var/log/aladdin/ear-agent` – журнал диагностики консольного агента сервера JMS;
- `/var/log/aladdin/ear-web-admin` – журнал диагностики серверного компонента консоли управления JMS;
- `/var/log/aladdin/jwa-service` – журнал диагностики JWA.

## 9. Обеспечение целостности и защиты от несанкционированного доступа файлов ПО JMS

Чтобы обеспечить целостность ПО JMS, директории для установки его компонентов не должны быть доступны пользователям, не являющимся администраторами сервера (хоста).

 **Примечание.** Директории для развертывания компонентов указываются в разделах настоящего документа с описанием установки продукта.

## 10. Настройка функций безопасности среды функционирования объекта оценки (JMS)

Для защиты информации, хранящейся в БД ПО JMS, следует установить и настроить наложенное криптографическое средство защиты информации (СКЗИ) «Крипто БД».

Установку и настройку СКЗИ «Крипто БД» для работы с JMS следует производить в соответствии разделом «Установка и настройка плагина СКЗИ «Крипто БД» для JMS», ниже.

Для обеспечения работы компонентов JMS, взаимодействующих с аппаратными средствами аутентификации и ЗНИ, требуется установка и настройка ПК «Единый Клиент JaCarta» [5].

В остальном объект оценки (JMS) не накладывает дополнительных требований к настройке среды функционирования.

Для управления настройкой элементов среды функционирования (операционных систем) объекта оценки следует использовать документацию из комплекта поставки данных ОС.

## 11. Установка и настройка плагина СКЗИ «Крипто БД» для JMS

СКЗИ «Крипто БД» предназначено для обеспечения конфиденциальности и контроля целостности информации, хранящейся в таблицах баз данных СУБД PostgreSQL, посредством криптографического преобразования и имитозащиты.

Использование наложенного сертифицированного СКЗИ «Крипто БД» для защиты таблиц БД JMS является обязательным для сертифицированной версии ПО JMS.

Для интеграции ПО JMS с СКЗИ «Крипто БД» выполните следующие шаги.

1. Выполните сборку и настройку pljava-расширения для СУБД PostgreSQL (см. «Приложение 3. Инструкция по сборке расширения pljava для СУБД PostgreSQL 9.6 под ОС Astra Linux», с. 100)
2. Установите плагины Крипто БД для сервера JMS:

```
sudo apt-get install ./aladdin-jms-cryptodb-server.4.1.0.xxxx_x64
```

3. Перезагрузите сервис JMS:

```
sudo systemctl stop eap-engine
sudo systemctl start eap-engine
```

4. Выгрузить текущую конфигурацию JMS при помощи команды консольного агента:

```
Aladdin.EAP.Agent.Terminal cryptodb config --path /tmp/EAPDB.xml
```

```
autotest@freeipa-orel:~$ Aladdin.EAP.Agent.Terminal cryptodb config --path /tmp/EAPDB.xml
Конфигурация КриптоБД выгружена в файл: /tmp/EAPDB.xml
autotest@freeipa-orel:~$
```

Рис. 24 – Индикация успешной выгрузки конфигурации Крипто БД в файл

5. Перед шифрованием базы данных выполните остановку сервиса JMS:

```
sudo systemctl stop eap-engine
```

6. В файле конфигурации postgresql.conf установите значение параметра:

```
standard_conforming_strings = on
```

7. Внесите дополнительные изменения в настройки ОС Astra Linux хоста, на котором установлен сервер СУБД PostgreSQL.  
В файле /etc/parsec/mswitch.conf установите zero\_if\_notfound: yes.
8. Перезагрузите сервис postgresql.
9. На подключенной к сети рабочей станции (или сервере) с ОС Windows установите инсталляционный пакет СКЗИ «Крипто БД»:  
*Aladdin.CryptoDB.Admin.Postgres.GOST\_7.0.0.XXX\_x64.msi*.  
Для уточнения процедуры установки следует использовать документацию СКЗИ «Крипто БД».
10. Из меню Пуск ОС Windows выполните запуск **Мастера Конфигурирования КриптоБД** выполните подключение к БД JMS на СУБД PostgreSQL.

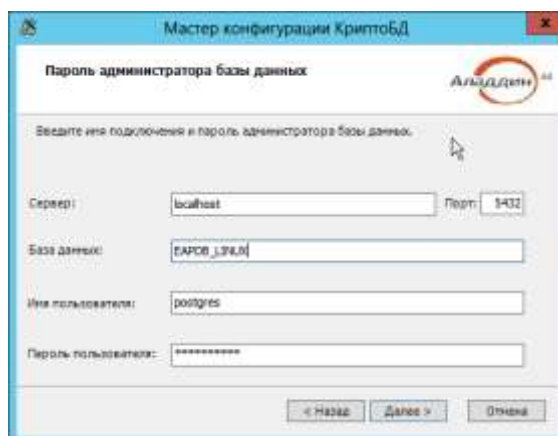


Рис. 25 – Мастер конфигурирования СКЗИ «Крипто БД»

11. Укажите опцию создания новой учетной записи администратора безопасности:

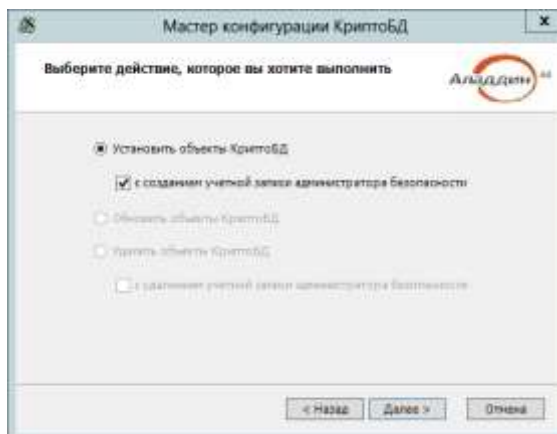


Рис. 26 – Окно выбора действия в конфигураторе СКЗИ «Крипто БД»

12. Введите имя администратора (например earpb\_admin), пароль и схему для хранения объектов «Крипто БД»:

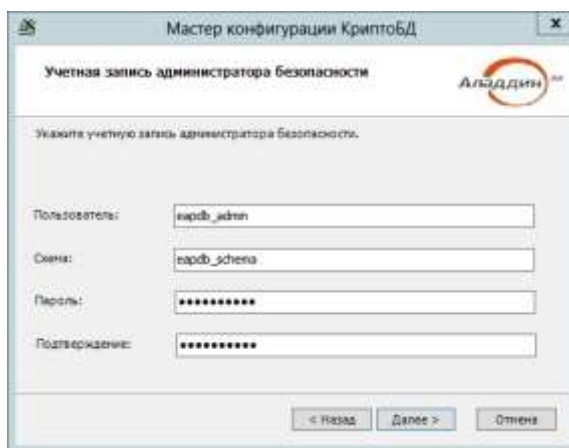


Рис. 27 – Окно создания учетной записи администратора безопасности СКЗИ «Крипто БД»

13. На следующем шаге укажите путь к **Файлу конфигурации**, выгруженному на шаге 4 (здесь – EAPDB.xml), и **Пароль сервера ключей** (пароль ключевого контейнера по умолчанию – 1234567890)

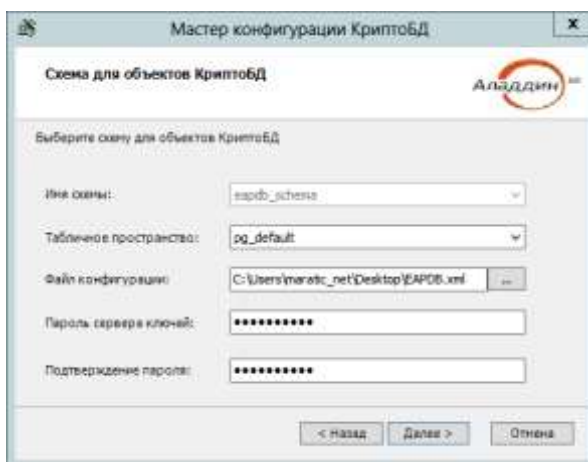


Рис. 28 – Окно формирования схемы объектов СКЗИ «Крипто БД» для БД IMS

#### 14. Выполните развертывание объектов «Крипто БД».


##### 14.1. На сервере СУБД подключитесь к БД JMS

```
sudo -u postgres psql -d <EAPDB>
```

где <EAPDB> – имя БД JMS.

##### 14.2. Предоставьте пользователю, созданному на шаге 12 (здесь – eapdb\_admin), права суперпользователя:

```
ALTER user eapdb_admin with superuser;
```

 **Примечание.** Данные права можно предоставить только на период выполнения операций шифрования таблиц БД JMS.

##### 14.3. В меню **Пуск** ОС Windows откройте **Администрирование КриптоБД Postgres**, подключитесь к БД JMS, указывая имя ранее созданного администратора безопасности:

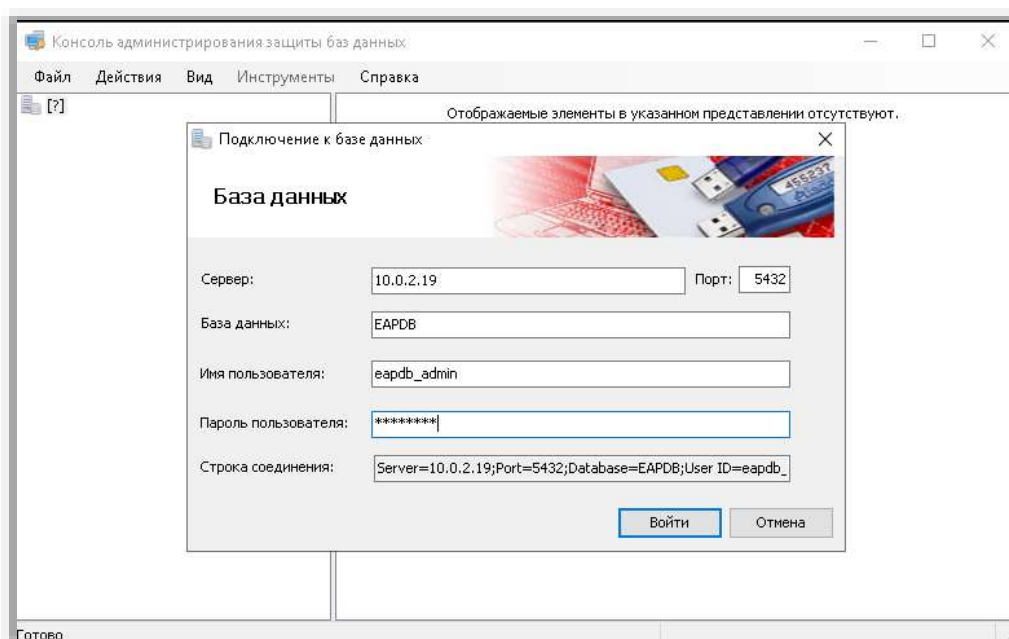


Рис. 29 – Подключение к БД JMS из консоли администрирования «Крипто БД»

##### 14.4. Выберите ключевой контейнер:

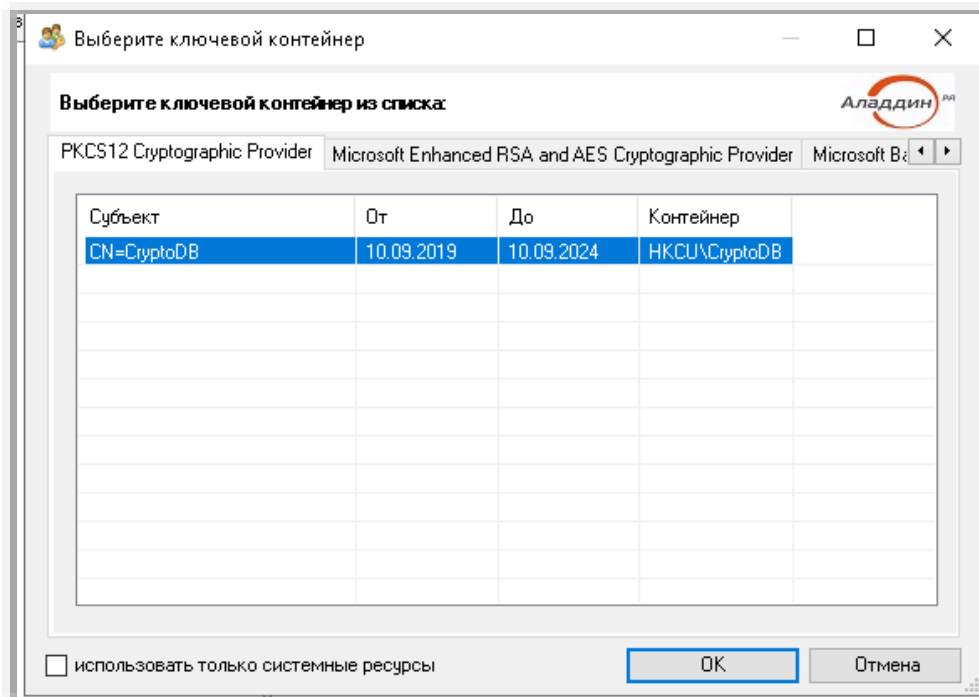


Рис. 30 – Выбор ключевого контейнера в консоли администрирования «Крипто БД»

14.5. В окне аутентификации введите пароль по умолчанию 1234567890:

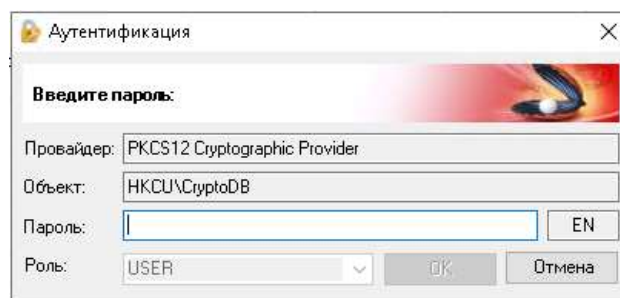


Рис. 31 – Ввод пароля ключевого контейнера



- 14.6. Перейдите в раздел **Настройки безопасности** -> **Сервер ключей**, по нажатию правой кнопки мыши выберите – **Запустить**. В появившемся окне нажмите **ОК** и введите заданный на шаге 13 **Пароль сервера ключей**:

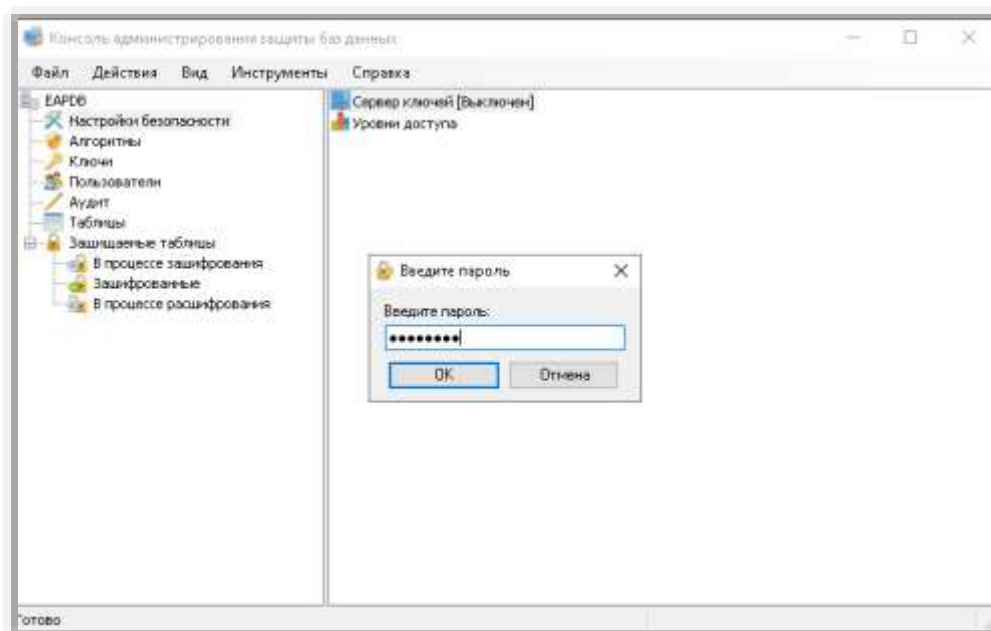


Рис. 32 – Ввод пароля сервера ключей

- 14.7. После ввода символов энтропии сервер ключей должен перейти в статус *Активен*.  
 14.8. В разделе **Защищаемые таблицы** -> **В процессе зашифрования** последовательно на каждой из таблиц по нажатию правой кнопкой мыши выбрать **Зашифровать**.

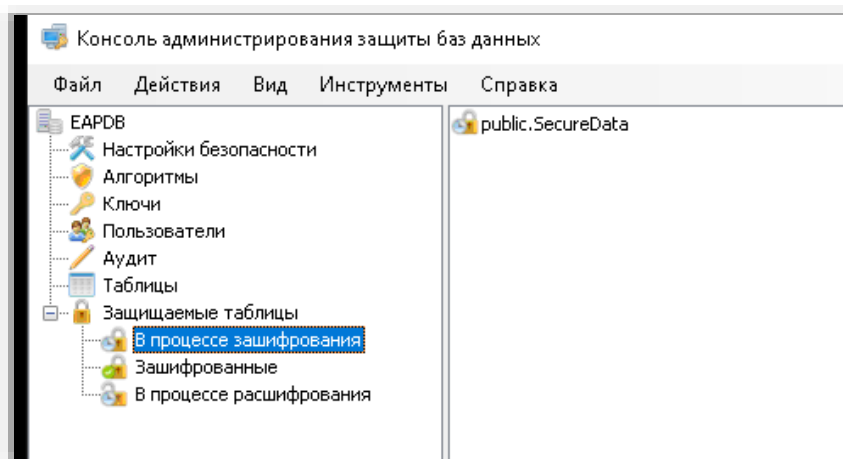


Рис. 33 – Выбор таблиц для зашифрования

- 14.9. Все шифруемые таблицы БД JMS (в соответствии со схемой защиты) должны появиться в разделе **Защищаемые таблицы -> Зашифрованные**:

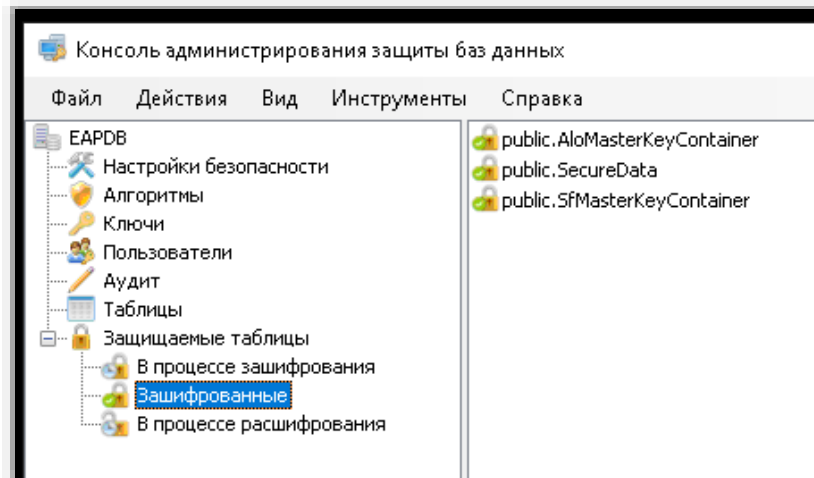


Рис. 34 – Проверка состава зашифрованных таблиц

15. Запустите сервис JMS:

```
sudo systemctl start eap-engine
```

16. При помощи консольного агента убедиться, что «Крипто БД» готова к работе – Сервер ключей КриптоБД должен быть запущен:

```
Aladdin.EAP.Agent.Terminal cryptodb status
```

```
autotest@freeipa-ore:~$ Aladdin.EAP.Agent.Terminal cryptodb status
Текущее состояние КриптоБД: Mounted (Сервер ключей КриптоБД запущен. Работа JMS с шифрованными данными разрешена)
autotest@freeipa-ore:~$
```

Рис. 35 – Индикация успешной загрузки сервера ключей Крипто БД

## 12. Утилита сбора диагностической информации о JMS

В состав каждого из компонентов JMS (сервера JMS, серверного web-приложения консоли управления) входит утилита сбора диагностической информации *Aladdin.EAP.DiagInfo.Terminal*, которая позволяет произвести диагностику установленного компонента (или всех установленных на данном хосте). Утилита устанавливается автоматически вместе с устанавливаемым компонентом из дистрибутива. Сбор диагностической информации упаковывается в архивный zip-файл с указанным местом расположения. Опционально предусмотрена генерация отчета о сборе диагностической информации.

Утилита служит для помощи в случаях сложного отказа системы с привлечением специалистов службы поддержки компании-производителя. По окончании процедуры сбора диагностической информации полученные файлы следует направить в службу поддержки компании «Аладдин».

Чтобы выполнить сбор диагностической информации, выполните следующие действия.

1. Проверьте корректность конфигурационного файла */opt/eap-diaginfo/Configuration/ProductConfiguration.json*, установленного по умолчанию:

```
[
  {
    "ProductName": "Aladdin R.D. JMS Server",
```

```

    "Path": "/opt/eap-engine",
    "LogConfigurationFile": "Aladdin.EAP.Engine.log4net",
    "OutputFormat": "Json",
    "ConfigFiles": [
        "*.config",
        "*.xml",
        "*.json",
        "/etc/aladdin/eap-engine/AppSettings.json"
    ]
  },
  {
    "ProductName": "Aladdin R.D. JMS Agent-Terminal",
    "Path": "/opt/eap-engine/eap-agent",
    "LogConfigurationFile": "Aladdin.EAP.Agent.Terminal.log4net",
    "OutputFormat": "Json",
    "ConfigFiles": [
        "*.config",
        "*.xml",
        "*.json"
    ]
  },
  {
    "ProductName": "Aladdin R.D. JMS Web Admin",
    "Path": "/opt/eap-web-admin",
    "LogConfigurationFile": "log4net.config",
    "OutputFormat": "Json",
    "ConfigFiles": [
        "*.config",
        "*.xml",
        "*.json"
    ]
  }
]

```

При необходимости внесите коррективы в конфигурационный файл. Описание параметров конфигурационного файла приведено в Табл. 9.

Табл. 9 – Параметры конфигурационного файла утилиты сбора диагностической информации

Параметр	Описание
<b>ProductName</b>	Наименование компонента продукта
<b>Path</b>	Путь к компоненту продукта
<b>LogConfigurationFile</b>	Путь к конфигурационному файлу подсистемы логгирования относительно пути к компоненту
<b>OutputFormat</b>	Тип конечных сериализуемых данных Json/XML (к примеру, информация об окружении)
<b>ConfigFiles</b>	Маска для определения конфигурационных файлов в папке с компонентом продукта, полный путь к конфигурационному файлу

- Запустите на выполнение утилиту диагностики (*Aladdin.EAP.DiagInfo.Terminal*) командой следующего вида.

```

sudo /opt/eap-diaginfo/Aladdin.EAP.DiagInfo.Terminal --zip /mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4LX_diags.zip --report /mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4LX_diags_report.txt

```

Ключи команды приведены в Табл. 10 (ниже).

В случае успешного выполнения производится выдача следующего вида.

```

-Aladdin R.D. JMS Web Admin
 1. Окружение - Выполнено
 2. Информация о файлах - Выполнено
 3. Конфигурационные файлы - Выполнено
 4. Лог-файлы - Выполнено

-Сохранение результатов
 1. Создание архива - Выполнено

Архив с данными диагностики сохранён по пути '/mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4
',
Отчёт сохранён по пути '/mnt/documents/JMS_4LX-Distrib/_diags/2021_09_01_JMS4LX_diags_report.txt'

```

Рис. 36 – Выдача утилиты сбора диагностической информации

Табл. 10 – Ключи команды *Aladdin.EAP.DiagInfo.Terminal* с примерами использования

Ключ команды	Описание	Обязателен	Значение ключа по умолчанию	Пример
--zip	Путь к конечному Zip-архиву	Нет	'<личная папка пользователя>/JMS Diagnostic Data/<yyyy.mm.dd_hh-mm>_DiagnosticData.zip'	--zip /home/admin/ diagnosticData.zip
--report	Путь к конечному файлу отчёта	Нет	Нет	--report /home/admin/diagnosticReport.txt

## 13. Сведения по запуску планов обслуживания из консольного агента JMS

План обслуживания - процедура, предназначенная для автоматизации массовых операций с объектами JMS, а также для выявления и устранения неполадок в работе JMS.

Подробное описание планов обслуживания JMS и порядка работы с ними из *консоли управления JMS* приведено во второй части руководства администратора [2], в разделе «Планы обслуживания».

В данном документе приводятся дополнительные сведения для запуска планов обслуживания из командной строки операционной системы (команда консольного агента *Aladdin.EAP.Agent.Terminal maintenance run*, подробнее см. в разделе «Приложение 2. Справочник команд консольного агента *Aladdin.EAP.Agent.Terminal*», с. 83), либо с помощью стандартных утилит-планировщиков заданий (см. «Настройка автоматического регулярного запуска планов обслуживания», ниже).

### 13.1 Автоматическая организация очередей выполнения заданий планов обслуживания

Команда *Aladdin.EAP.Agent.Terminal maintenance run* позволяет организовывать очередь выполнения заданий планов обслуживания. Очередь организуется в порядке поступления заявок на выполнение (в порядке последовательных запусков команды *maintenance run*).

При этом в очередь могут быть поставлены несколько заданий на выполнение одного и того же плана обслуживания (например с разными параметрами).

## 13.2 Настройка автоматического регулярного запуска планов обслуживания

Для чтобы настроить автоматический запуск плана обслуживания по расписанию следует воспользоваться утилитой планирования заданий (например стандартным демоном cron ОС Linux).

В настройках планировщика заданий (например, в файле *crontab*) следует указывать команду консольного агента *Aladdin.EAP.Agent.Terminal maintenance run* (описание параметров приведено в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83).

### 13.2.1 Пример добавления задания в crontab на выполнение плана обслуживания

Запуск планов обслуживания JMS в cron рекомендуется осуществляется посредством bash-скриптов, в которых обеспечивается аутентификация пользователя JMS с ролью *Запуск планов обслуживания*.

Для добавления задания на выполнение плана обслуживания произведите следующие действия.

1. Создайте файл пароля пользователя JMS, имеющего права на *Запуск планов обслуживания*, разместив его в защищённом каталоге, например в личном каталоге пользователя данного хоста (сервера JMS). Данную операцию можно выполнить, например, следующей командой (из личного каталога пользователя, например /home/user)

```
echo PASSWORD > ./secret_password
```

где:

**PASSWORD** -- значение доменного пароля пользователя JMS с ролью *Запуск планов обслуживания*;

**secret\_password** -- файл со строкой пароля.


2. Создайте файл bash-сценария (например */var/jms\_scripts/script.sh*), для выполнения плана обслуживания, например, следующего содержания:

```
#!/bin/bash
# строка выше это шебанг который среда использует для автоопределения оболочки, в
которой запускать скрипт.
# В переменную PASS устанавливаем содержимое файла с паролем, который создали ранее
PASS=$(cat /home/user/secret_password)
# Через консольный агент JMS вызываем команду аутентификации доменного пользователя
с правами JMS на запуск планов обслуживания
Aladdin.EAP.Agent.Terminal auth --login 'FQDN\USERLOGIN' --password $PASS
# Вызываем запуск плана обслуживания согласно полученной команде из UI WebAdmin.
eap-agent maintenance run -g 553aa527-94c4-40ef-84be-1de5b4bfb7a7 -p
Operations="EAP_CLEAR_GROUP_CACHE, EAP_ACCOUNT_SYNCHRONIZATION, EAP_CHECK_LICENSE,
EAP_CHECK_PROFILES, EAP_CHECK_ROLES, EAP_CHECK_TEMPORARY_USER_ACCESS,
EAP_SECURE_PROFILES, EAP_CHECK_CRYPTO_DEVICE, EAP_CHECK_TOKEN_DOCUMENTS,
EAP_LOG_ROTATION, EAP_REFRESH_TOKEN_CLEANER"
```

где:

`/home/user/secret_password` -- файл с паролем пользователя, созданным на шаге 1;

`FQDN\USERLOGIN` -- доменное имя пользователя JMS с ролью *Запуск планов обслуживания* в формате `<FQDN-имя_домена>\<логин_пользователя>`, например: `jms4.local\admin`

 **Примечание.** В приведенном примере подсказки-UI WebAdmin для запуска плана обслуживания с помощью команды консольного агента `maintenance run` используется алиас `eap-agent`, который в некоторых конфигурациях операционных систем Linux может интерпретироваться с ошибками. В этом случае его следует заменить полной командой вызова консольного агента `Aladdin.EAP.Agent.Terminal` (в приведенном примере это будет: `Aladdin.EAP.Agent.Terminal maintenance run ...`)

3. Присвойте права на выполнение созданного скрипта для пользователя, от имени которого он был создан (в нашем случае локальный пользователь `user`), для возможности его запуска из планировщика `cron`:

```
chmod u+x /var/jms_scripts/script.sh
```

4. В файл `/etc/crontab` добавьте правило (строку в конец файла) с запуском подготовленного сценария `script.sh`, например такое:

```
0 */12 * * * sudo user /var/jms_scripts/script.sh
```

 **Примечания:**

1. Для запуска приведенного в примере правила необходимо, чтобы пользователь, от имени которого запускается задание (в нашем примере -- `user`), состоял в группе `astra-admin`.
2. В самом правиле, как указано в примере, сценарий должен запускаться с повышением привилегий пользователя с помощью `sudo`.
3. Приведенное в качестве примера `crontab`-правило означает следующее: запускать `bash`-сценарий от имени локального пользователя `user` раз в 12 часов, независимо от числа, месяца и дня недели).

### 13.3 Автоматическая генерация параметров запуска команды `maintenance run`

При работе с консолью управления JMS (см. руководство по функциям управления JMS [2]) в некоторых планах обслуживания, предусматривающих выбор ресурсной системы и ее контейнера, администратору предоставляется сервис автоматической генерации параметров запуска команды консольного агента `Aladdin.EAP.Agent.Terminal maintenance run`.

Для получения таких параметров выполните следующие действия (приведены на примере **Плана обслуживания пользователей**).

1. Запустите план обслуживания на выполнение. Для этого в разделе **Планы обслуживания** выберите соответствующий план (например, **План обслуживания пользователей**), нажмите на нём правой кнопкой мыши и выберите **Запустить**. Отобразится окно следующего вида:

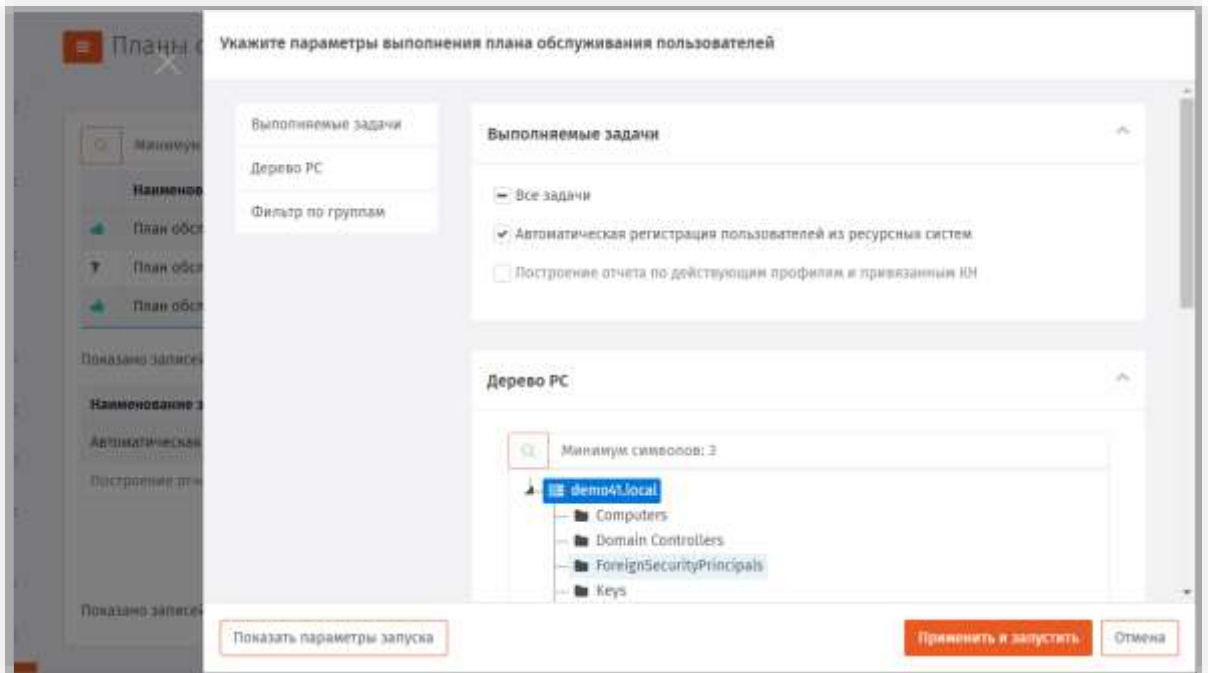


Рис. 37 – Окно выбора контейнера ресурсной системы для применения плана обслуживания

2. Выберите контейнер ресурсной системы (например, **Users**) и нажмите **Показать параметры запуска**.  
Отобразится окно следующего вида.

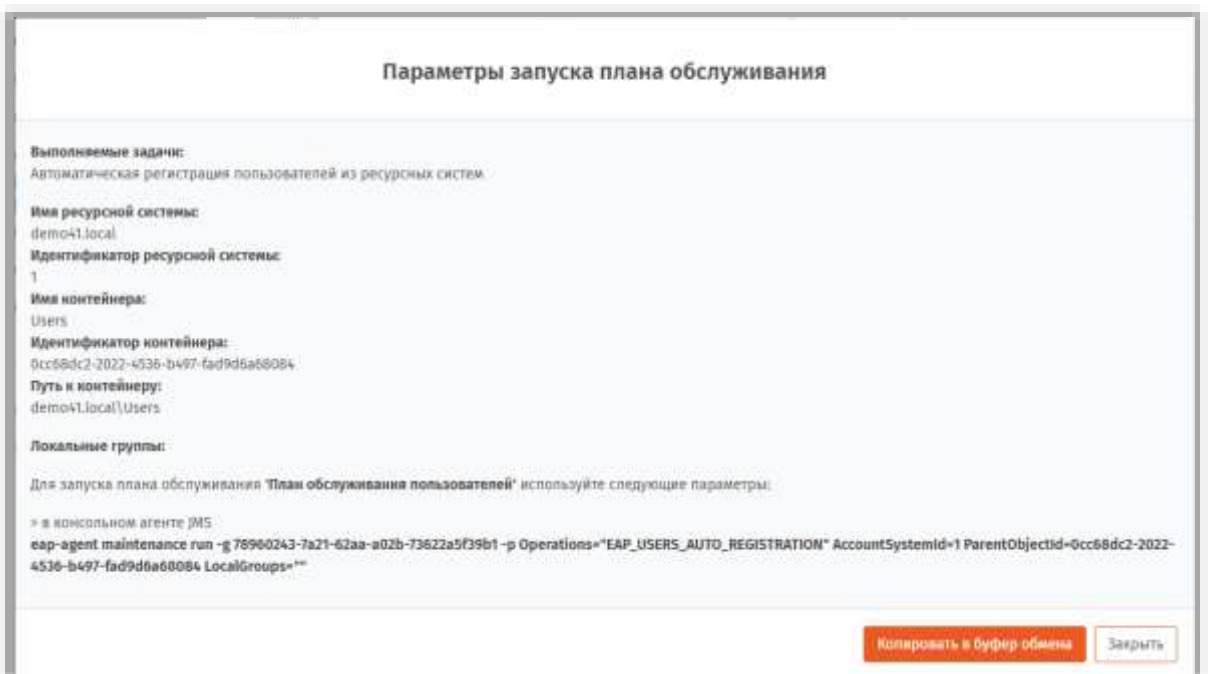


Рис. 38 – Окно с готовыми параметрами запуска команды *Aladdin.EAP.Agent.Terminal maintenance run*

Предложенную строку параметров команды консольного агента *Aladdin.EAP.Agent.Terminal maintenance run* можно скопировать в буфер обмена и использовать для запуска выбранного плана обслуживания из командной строки или с помощью утилиты-планировщика заданий.

**Примечание.** В указанном примере (Рис. 38) вместо вызова терминального агента (Aladdin.EAP.Agent.Terminal) используется его псевдоним (eap-agent). Если в вашей операционной системе или среде исполнения не поддерживается использование псевдонима, то команду `eap-agent maintenance run` следует заменить на `Aladdin.EAP.Agent.Terminal maintenance run`.

## 14. Добавление поддержки моделей ЭК / профилей в JMS

Для добавления поддержки моделей ЭК и соответствующих им профилей (отсутствующих в конфигурации JMS по умолчанию) следует воспользоваться командой консольного агента `Aladdin.EAP.Agent.Terminal applet enable` (подробное описание команды `applet enable` см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83).

Например, чтобы подключить поддержку ЭК **eToken Pro (Java) / JaCarta PRO** выполните команду:

```
Aladdin.EAP.Agent.Terminal applet enable 4
```

```
root@lx-jms4:/var/jms4/distr# Aladdin.EAP.Agent.Terminal applet enable 4
Приложение ProJava теперь включено.
```

Рис. 39 – Пример выдачи команды `Aladdin.EAP.Agent.Terminal applet enable`

**Примечание.** В процессе выполнения команды после подключения нового приложения выполняется автоматический перезапуск сервера JMS.

После добавления поддержки нового типа электронного ключа в консоли управления добавится соответствующий профиль инициализации ЭК (в приведенном примере – профиль **eToken Pro (Java) / JaCarta PRO**)

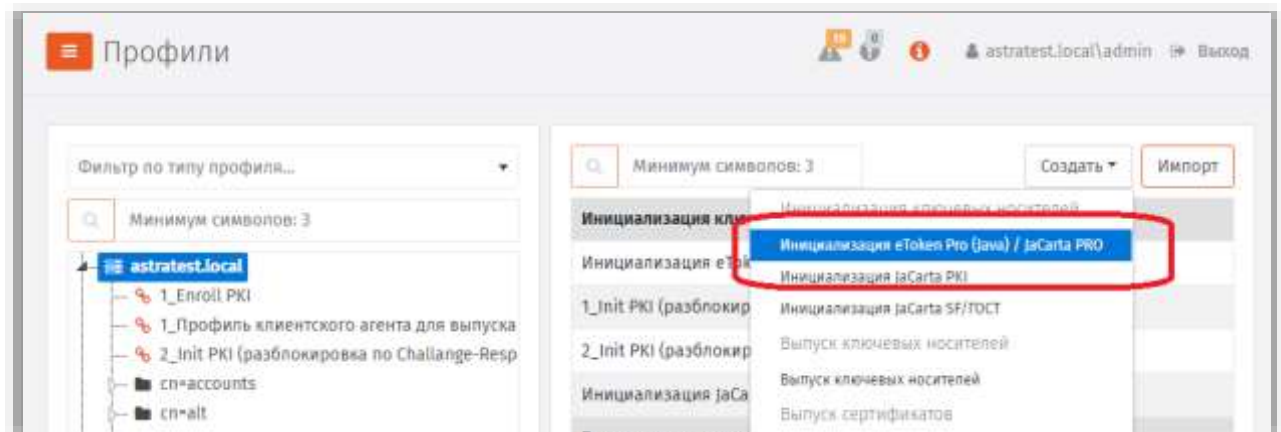


Рис. 40 – В JMS добавлен профиль для ЭК eToken Pro (Java) / JaCarta PRO

## 15. Установка коннектора к Offline Certification Authority

Коннектор к Offline Certification Authority представляет собой компонент JMS, который позволяет выполнять выпуск сертификатов пользователей в аккредитованных удостоверяющих центрах, не имеющих сетевого подключения к телекоммуникационным сетям общего пользования.

**Примечание.** Компонент «Коннектор к Offline Certification Authority» является лицензируемой опцией продукта JMS. Функциональность компонента доступна только при условии приобретения соответствующей опции, информации о которой зафиксирована в файле лицензии на продукт.



### 15.1 Дистрибутив

Дистрибутив коннектора к Offline Certification Authority включает следующие пакеты установки (Табл. 11).

Табл. 11 – Дистрибутив коннектора к Offline Certification Authority

ОС	Файл дистрибутива	Описание
Astra Linux	<b>aladdin-jms-offline-ca-adapter-server_x.x.x.xxxx-x64.deb</b>	Коннектор к Offline Certification Authority
РЕД ОС, ОС Альт	<b>aladdin-jms-offline-ca-adapter-server_x.x.x.xxxx-x64.rpm</b>	

### 15.2 Системные требования коннектора к Offline Certification Authority

Требования к среде функционирования компонента коннектора к Offline Certification Authority приведен в Формуляре [4].

### 15.3 Порядок установки коннектора к Offline Certification Authority

#### 15.3.1 Подготовительные действия

Скопируйте с дистрибутивного диска на целевую машину с ОС Linux, предназначенную для установки коннектора, файл дистрибутива

#### 15.3.2 Установка



**Примечания:**

- Все команды в данном разделе выполняются в контексте пользователя root.
  - Установка описывается на примере дистрибутива для ОС Astra Linux.
1. Установите компонент «Коннектор к Offline Certification Authority», выполнив следующую команду

```
dpkg -i /var/jms4/distr/ aladdin-jms-offline-ca-adapter-server_4.0.0.5300_x64.deb
```

По окончании успешной установки должна отобразиться информация следующего вида:

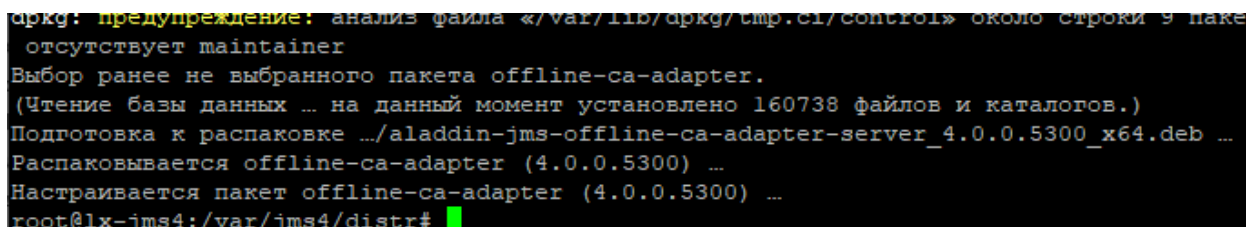



Рис. 41 – Информация в консоли в случае успешной установки компонента «Коннектор к Offline Certification Authority»

2. Выполните команду инициализации компонента:

```
Aladdin.EMS.OfflineCertAuthority initialize
```

 **Примечание.** Для получения полного перечня команд коннектора обратитесь к разделу «Приложение 4. Справочник команд коннектора к Offline Certification Authority», с. 104.

Отобразится запрос аутентификационной информации.

```
root@lx-jms4:/var/jms4/distr# Aladdin.EMS.OfflineCertAuthority initialize
2021-11-24 14:41:58,814 [1] GetControlManager => ControlApiUrl = 'http://localhost:8119'
2021-11-24 14:41:58,850 [1] GetAuthenticationManager => AuthApiUrl = 'http://localhost:8121'
2021-11-24 14:41:59,116 [1] Try execute GetAuthDataByCustomCredentials
2021-11-24 14:41:59,117 [1] Try execute GetAuthDataByEnteredCredentials
Login:

```

Рис. 42 – Запрос аутентификационной информации

3. На запрос **Login** введите логин пользователя в формате:  
    <имя\_ресурсной\_системы>\<имя\_пользователя>,  
    где <имя\_ресурсной\_системы> – значение, указанное в поле [accountSystem] -> name  
    файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной  
    конфигурации сервера JMS», с. 78).  
    Например:

```
DirectoryAlias\admin
```

 **Примечание.**

Альтернативным способом аутентификации пользователя является указание в качестве доменного префикса:

- для **AD** и **SambaAD**: netbios-имени домена. Например для домена aladdin.local и пользователя admin допускается ввести значение aladdin\admin
- для **FreelPA**: полного или FQDN-имени домена. Например для домена astratest.local и пользователя admin допускается ввести значение astratest.local\admin

4. На запрос **Password** введите пароль пользователя.
5. В процессе инициализации будет автоматически перезапущен сервер JMS.  
По окончании успешного выполнения команды должна отобразиться информация следующего вида:

```
2021-11-24 14:47:38,105 [1] GetProfileAction: Create
2021-11-24 14:47:38,105 [1] InitialConfigurationRegisterProfile <<<
2021-11-24 14:47:40,171 [1] No profile updates needed. Finishing installation.
root@lx-jms4:/var/jms4/distr#
```

Рис. 43 – Выдача по окончании инициализации компонента

- Б. Для проверки корректности функционирования компонента «Коннектор к Offline Certification Authority» откройте web-интерфейс *Консоли управления JMS* и в разделе **Профили** нажмите **Создать**.

В открывшемся меню выбора профилей должно отобразиться меню, содержащее пункт **Выпуск сертификатов (режим офлайн)** (Рис. 44) в секции **Выпуск сертификатов**.

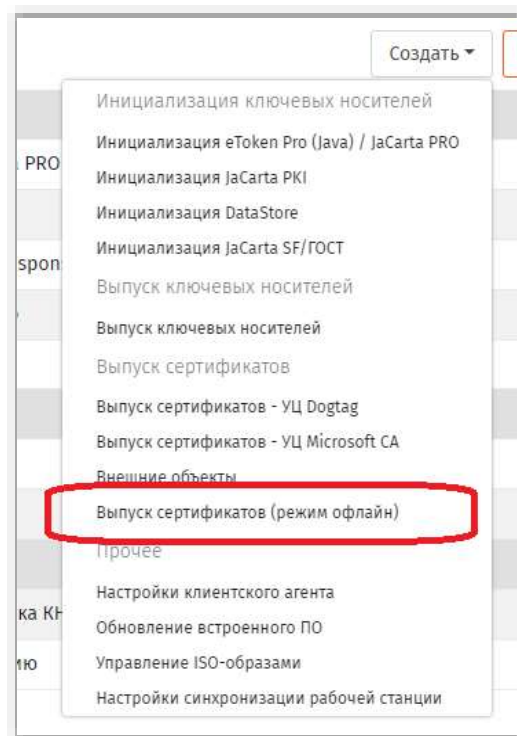



Рис. 44 – Пример корректного подключения шаблона профиля **Выпуск сертификата (режим офлайн)**

## 15.4 Порядок удаления коннектора к Offline Certification Authority

Для удаления коннектора выполните следующую команду:

```
sudo dpkg -r offline-ca-adapter
```

 **Примечание.** При обновлении JMS удаление коннектора следует производить перед удалением сервера JMS.

## 16. Установка Прокси-сервера для УЦ (Web API к УЦ)

Компонент *Прокси-сервер для УЦ* (Certification Authority Proxy Service) или *Web API к УЦ* предназначен для обеспечения взаимодействия с удостоверяющим центрами, для которых на данный момент не предусмотрено непосредственных API-интерфейсов для JMS.

В текущей реализации данный Прокси-сервер обеспечивает взаимодействие JMS с УЦ Microsoft Certification Authority. При этом настройка взаимодействия обеспечивается через стандартный профиль JMS для выпуска сертификата через MSCA.

Прокси-сервер устанавливается на Windows-хосте, функционирующем в одном домене с сервером Microsoft, на котором развернута ролевая служба Certification Authority.

## 16.1 Дистрибутив

Дистрибутив Прокси-сервера для УЦ MSCA включает следующие пакеты установки (Табл. 12).

Табл. 12 – Дистрибутив Прокси-сервера для УЦ MSCA

ОС	Файл дистрибутива	Описание
64-битная платформа Microsoft Windows	Aladdin.CAProxyService-x.x.x-x64.msi	Прокси-сервер для УЦ MSCA

## 16.2 Системные требования Прокси-сервера для УЦ MSCA

Минимальные системные требования:

- Серверные ОС Windows Server 2012 R2 и выше
- Клиентские ОС Windows 10 и выше (требуется установка компонента RSAT: Active Directory Certificate Services Tools)
- .NET Framework 4.8

## 16.3 Порядок установки Прокси-сервера для УЦ MSCA

### 16.3.1 Подготовительные действия

Скопируйте с дистрибутивного диска на целевую машину с ОС Windows, предназначенную для установки прокси-сервера, файл дистрибутива

### 16.3.2 Установка

Чтобы установить компонент Прокси-сервера для УЦ MSCA, выполните следующие действия.

1. Запустите на выполнение файл инсталлятора *Aladdin.CAProxyService-1.0.0.4-x64.msi*:

Отобразится следующее окно.

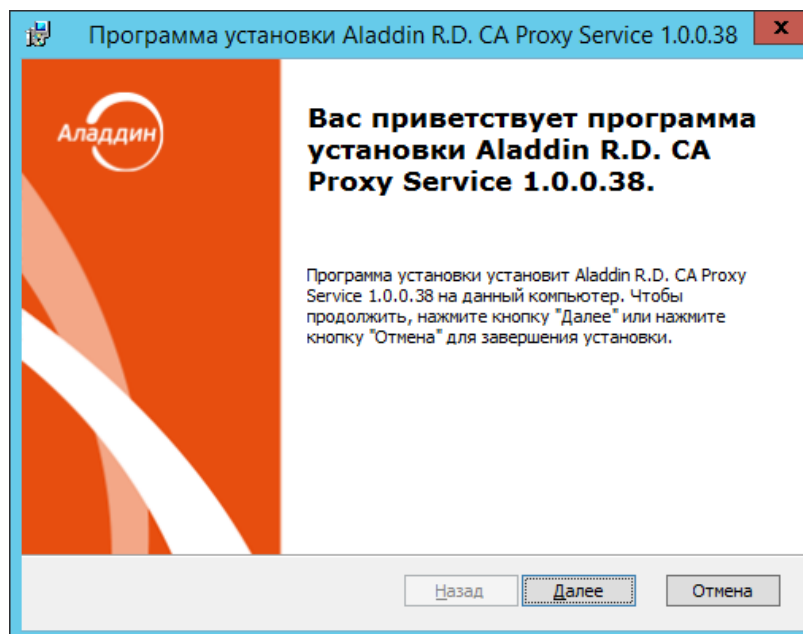


Рис. 45 – Окно приветствия мастера установки Прокси-сервера для УЦ MSCA

2. Нажмите **Далее**. Отобразится окно лицензионного соглашения. Выберите **Я принимаю условия лицензионного соглашения**, нажмите **Далее** и следуйте указаниям мастера до полной установки Прокси-сервера для УЦ MSCA.

По завершении установки отобразится следующее окно.

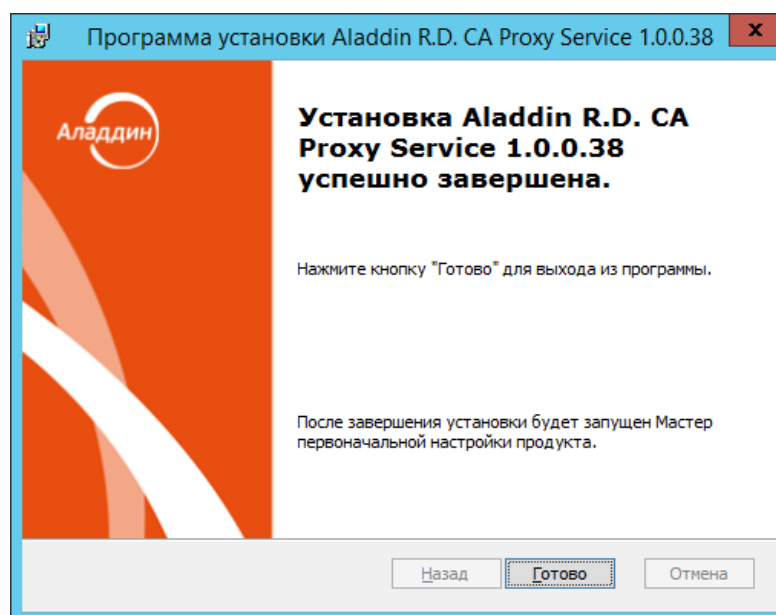


Рис. 46 – Окно завершения процедуры установки

По окончании установки в системе должен появиться новый запущенный Windows-сервис с именем **CAProxySvc\_default (CA Proxy Service - default)**, Рис. 47.

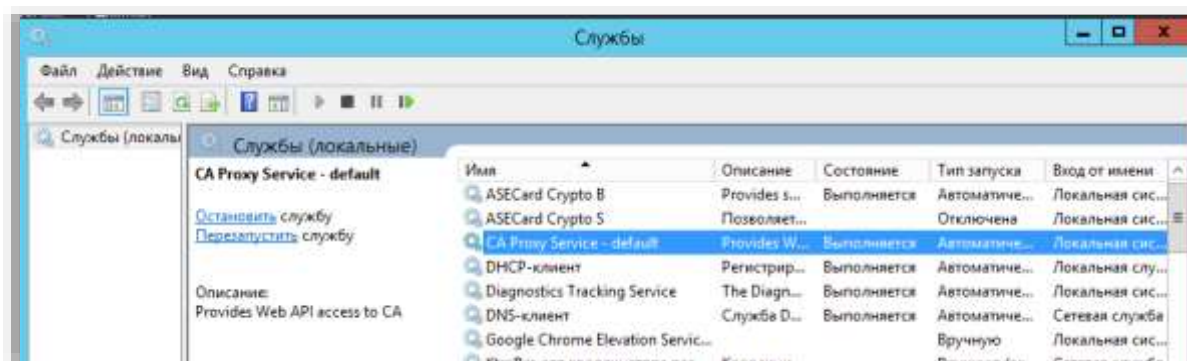


Рис. 47 – Отображение установленного сервиса для Web API

## 16.4 Первичная проверка работы Прокси-сервера для УЦ MSCA

Проверить работу сервиса можно запустив в браузере следующий URL и пройдя аутентификацию:

<http://localhost:6610/api/ca/ping>

В ответ система должна вернуть строку следующего вида (Рис. 48).

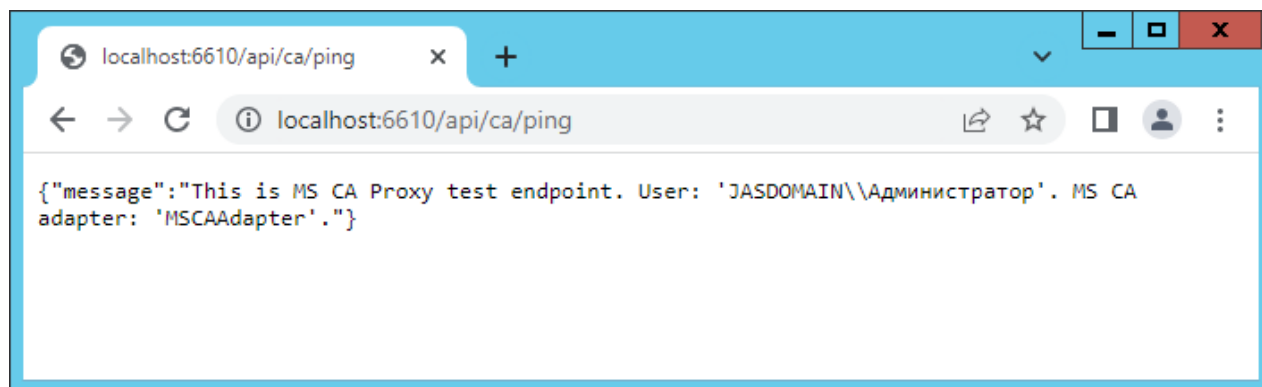


Рис. 48 – Отображение ответа Web API на тестовый запрос

## 16.5 Настройки Прокси-сервера для УЦ MSCA

После завершения процедуры установки может потребоваться дополнительная настройка сервиса, описанная в настоящем подразделе. Настройка может выполняться через реестр и/или конфигурационные файлы. После любых изменений настроек требуется перезапуск сервиса, который выполняется последовательностью команд:

```
net stop CAProxySvc_default
net start CAProxySvc_default
```

## 16.6 Настройка подключения к УЦ

Дополнительных настроек для подключения к УЦ не предусмотрено – Прокси-сервер автоматически использует все доступные УЦ.

## 16.7 Настройка полномочий на MSCA для доменного компьютера – прокси-сервера

Для обеспечения возможности доступа прокси-сервера к шаблонам сертификатов, данному доменному компьютеру (с установленным Прокси-сервером для УЦ MSCA) следует предоставить полные права на доступ к шаблонам сертификатов, которые планируется выпускать с помощью JMS.

Для предоставления таких прав воспользуйтесь оснасткой «Центр Сертификации» (Certification Authority) на сервере с ролью MSCA.

Порядок подготовки и регистрации шаблонов сертификатов MSCA можно изучить на примере подготовки шаблона сертификата пользователя в специальном руководстве по шаблонам сертификатов [7], с.114, в таких разделах, как:

- «Шаблон сертификата для пользователей JMS»;
- «Шаблон сертификата агента регистрации»;



**Примечание.** При создании шаблона «Агент регистрации JMS» в дополнение к приведенной в указанном документе инструкции в свойствах шаблона на вкладке **Обработка запроса** следует установить флаг **Разрешить экспортировать закрытый ключ**, поскольку по технологии настройки данный сертификат экспортируется на сервер JMS с закрытым ключом.

## 16.8 Настройка адресов и портов

По умолчанию Прокси-сервер поднимает две точки входа с базовыми адресами <http://localhost:6610> и <https://localhost:6611> для подключения по HTTP и HTTPS. При необходимости можно изменить базовый адрес сервиса в следующем разделе реестра:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Aladdin\CA Proxy Service\MSCAProxyWebApi]

Для задания адресов используется строковый параметр **MSCAProxyWebApiAddresses**.

В качестве значения параметра следует указать список базовых адресов через точку с запятой. Поддерживается указание адресов в виде IP, имени хоста, \* (любой хост) или localhost (для локальных подключений), например:

**MSCAProxyWebApiAddresses** = [http://\\*:6610](http://*:6610);<https://localhost:6611>

Используемые порты должны быть доступны извне через межсетевой экран.

## 16.9 Настройка SSL

Для настройки подключения по https необходимо предварительно выполнить привязку порта к SSL-сертификату для приложения, выполнив команду следующего вида:

```
netsh http add sslcert ipport=0.0.0.0:6611
certhash=6A1F7A11447CD6D249FE093233E57B1AA1E76033 appid={ 670f608f-28ad-4724-8264-
7b3c0eb2dfd6}
```

Сам SSL-сертификат необходимо установить в хранилище компьютера (Machine Store).

## 16.10 Настройка аутентификации и авторизации

Прокси-сервер поддерживает Basic- и NTLM-аутентификацию.

Дополнительно можно включить авторизацию по доменной или локальной группе. Настройка выполняется в разделе реестра:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Aladdin\CA Proxy Service\MSCAProxyWebApi]

Для настройки используйте строковый параметр **MSCAProxyWebApiAddresses**.

В качестве значения параметра следует указать локальную или доменную группу, в которой должен состоять пользователь для выполнения операций через прокси-сервер. Например:

**AuthorizeAsGroupMember** = CA\_PROXY\_GROUP

По умолчанию авторизация отключена (т.е. параметр **AuthorizeAsGroupMember** не задан)

Для указания хранилища, в котором будет находиться группа используйте строковый параметр **AuthorizationGroupStore**.

В качестве значения указываются домен контроллер (по умолчанию) или локальный компьютер:

**AuthorizationGroupStore** = Domain

или

**AuthorizationGroupStore** = Machine

### 16.11 Настройка локализации

Прокси-сервер поддерживает два языка – русский (по умолчанию) и английский. Переключение языка осуществляется следующей настройкой реестра:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Aladdin\CA Proxy Service\Settings]

**Culture** = ru

или

**Culture** = en

### 16.12 Настройка работы прокси на клиентских операционных системах

Для корректной работы Прокси-сервера на клиентских операционных системах Windows 10 и более поздних необходимо установить специальный компонент *RSAT: Active Directory Certificate Services Tools*.

Чтобы установить RSAT в Windows 10, необходимо перейти в **раздел Settings -> Apps -> Manage Optional Features -> Add a feature (Параметры Windows -> Приложения -> Дополнительные возможности -> Добавить компонент)**.

В списке выбрать и установить компонент RSAT: Active Directory Certificate Services Tools:

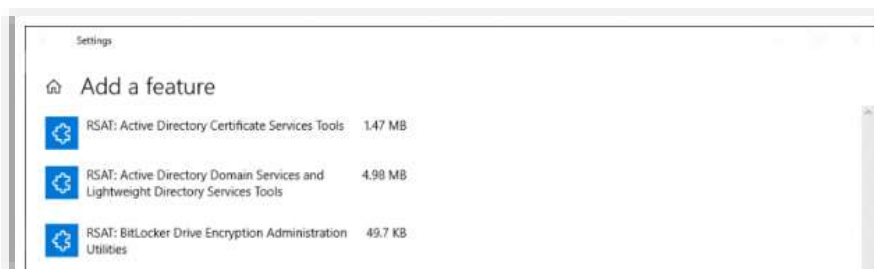


Рис. 49 – Выбор компонента RSAT: Active Directory Certificate Services Tools

Дополнительную информацию см. по адресу: <https://winitpro.ru/index.php/2018/10/04/ustanovka-rsat-v-windows-10-iz-powershell/>

### 16.13 Журналы диагностики Прокси-сервера для УЦ MSCA

Настройки журналов диагностики Прокси-сервера для УЦ MSCA задаются в конфигурационном файле:

C:\Program Files\CA Proxy Service\Aladdin.CAProxyService.log4net



По умолчанию журнал диагностики записывается в DEBUG-режиме в следующий каталог:

```
C:\ProgramData\Aladdin\CA Proxy Service\Logs
```

Одновременно ведется запись важных событий в журналы ОС Windows (Windows Event Log):

**Журналы приложений и служб -> CA Proxy Service (Applications and Services Logs -> CA Proxy Service)**

## 16.14 Настройка сервера JMS для работы с Прокси-сервером для УЦ MSCA

Для подключения JMS к Прокси-серверу для УЦ MSCA выполните следующие настройки.

1. На стороне УЦ MSCA выпустите сертификат Enrollment Agent (компьютер) с установленной опцией экспорта закрытого ключа (подробнее см. в разделе «Настройка полномочий на MSCA для доменного компьютера – прокси-сервера», с. 54).
2. Экспортируйте сертификат Enrollment Agent в pfx-файл с паролем.
3. На сервере JMS выполнит импорт сертификата командой следующего вида:

```
sudo Aladdin.EAP.Agent.Terminal certificates install --path /EnrollmentAgent.pfx --password simsim
```

4. Убедитесь в корректной установке сертификата в хранилище пользователя root с помощью команды консольного агента:

```
sudo Aladdin.EAP.Agent.Terminal certificates list
```

При этом будут отображены сертификаты из хранилища 'My' (расположение: CurrentUser).  
Например:

```
Отпечаток сертификата: 4B69444FC5A307BECC2DC49CF1771A06BE5DE919 Наименование: SN: CN=TESTSQL2017.fqdn5.com
Отпечаток сертификата: 04FC318611877FF139B75F80F4B4C164251E58EF Наименование: SN: CN=KRIS.MAC.local
Готово.
```

5. Экспортируйте корневой сертификат УЦ MSCA в формат cer (DER).
6. Сконвертируйте корневой сертификат УЦ MSCA в формат crt – например при помощи пакета openssl:

```
openssl x509 -inform DER -in <filepath>/CA-Root.cer -out CA-Root.crt
```

7. Добавьте полученный crt-сертификат в список доверенных. Данная процедура варьируется в зависимости от типа операционной системы хоста. Например:

7.1. В случае Astra Linux:

- 7.1.1. Скопируйте полученный crt-файл в директорию /usr/local/share/ca-certificates/
- 7.1.2. Выполните команду

```
sudo update-ca-certificates
```

7.2. В случае РЕД ОС:

- 7.2.1. Установите пакет ca-certificates:

```
yum install ca-certificates
```

- 7.2.2. Установите опцию динамической конфигурации:

```
update-ca-trust force-enable
```

7.2.3. Добавьте файл сертификата в каталог /etc/pki/ca-trust/source/anchors/:

```
cp CA-Root.crt /etc/pki/ca-trust/source/anchors/
```

7.2.4. Выполните команду:

```
update-ca-trust extract
```

Аналогичную инструкцию по добавлению crt-сертификата в список доверенных для других ОС можно найти по этой ссылке:

<https://manuals.gfi.com/en/kerio/connect/content/server-configuration/ssl-certificates/adding-trusted-root-certificates-to-the-server-1605.html>

После этих настроек JMS готов к работе с УЦ через прокси-сервер.

## 17. Подготовка к использованию протоколов SSL/TLS

Для обеспечения поддержки защищенных протоколов SSL/TLS необходимо выполнить ряд настроек как на стороне сервера JMS, так и в других компонентах системы (Рис. 50).

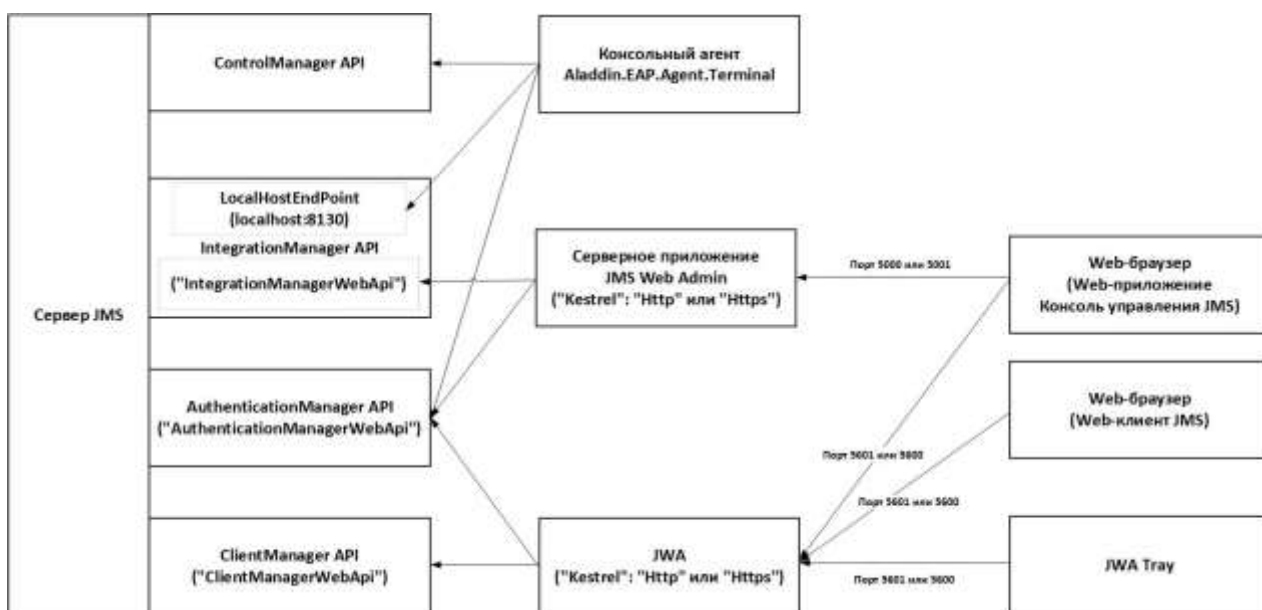


Рис. 50 – Схема настройки SSL на API-интерфейсах компонентов JMS

### 17.1 Настройка SSL-соединения на стороне сервера JMS

Для включения SSL на интерфейсах сервера JMS следует использовать команду `ssl enable` консольного агента `Aladdin.EAP.Agent.Terminal`. Например:

```
Aladdin.EAP.Agent.Terminal ssl enable --path /opt/41/f_pfx/ssl.pfx --password P@ssw0rd
```

В результате успешной настройки конфигурации на консоли отобразится:

```
root@jms4lastral7:/mnt/documents/back_to_share/cert# Aladdin.EAP.Agent.Terminal ssl enable --path /opt/tl/f_gfa/ssl.pem --password P@ssw0rd
Тип Api не указан, используется значение по умолчанию (all).
Остановка сервера...
Запуск EAP-сервиса...
EAP-сервис запущен.
Текущее состояние сервера: Работает
root@jms4lastral7:/mnt/documents/back_to_share/cert#
```

Рис. 51 – Выдача команды настройки SSL на API-интерфейсах сервера JMS

В приведенном примере используется ssl-сертификат сервера JMS и настройка осуществляется одновременно на интерфейсах IntegrationManager API (интерфейс взаимодействия с Консолью управления JMS) и ClientManager API (интерфейс взаимодействия с клиентскими компонентами JWA). Команда предусматривает также возможность устанавливать SSL отдельно на каждом из указанных интерфейсов, а также использовать уже ранее установленный в системе сертификат.

Подробное описание команды `ssl enable` ее см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83.

Для проверки текущей настройки SSL на интерфейсах Сервера JMS используйте команду консольного агента `ssl show`, например:

```
Aladdin.EAP.Agent.Terminal ssl show
```

```
root@jms4lastral7:/etc/aladdin/eap-engine# Aladdin.EAP.Agent.Terminal ssl show
Административный интерфейс (integration):
  Адрес: https://*:8120
  Отпечаток сертификата: 0205B30A4744493A5D2CB6356953B494840F6632
Клиентский интерфейс (client):
  Адрес: https://*:8122
  Отпечаток сертификата: 0205B30A4744493A5D2CB6356953B494840F6632
root@jms4lastral7:/etc/aladdin/eap-engine#
```

Рис. 52 – Пример выдачи команды `ssl show`

## 17.2 Настройка SSL/TLS на стороне Web-приложения Консоль управления JMS

Для обеспечения функционирования web-консоли управления JMS внесите следующие правки в конфигурационный файл `/etc/aladdin/eap-web-admin/appsettings.json`

1. Укажите адрес для защищенного подключения к API управления сервером JMS:

```
"WebAdminSettings": {
  "IntegrationApiUrl": "https://<FQDN_Сервера_JMS>:8120",
```

Где `<FQDN_Сервера_JMS>` -- полное доменное имя сервера JMS.

2. Укажите адрес для защищенного подключения к API аутентификации сервера JMS:

```
"WebAdminSettings": {
  "AuthenticationApiUrl": "https://<FQDN_Сервера_JMS>:8121",
```

Где `<FQDN_Сервера_JMS>` -- полное доменное имя сервера JMS.

3. Для безопасного подключения к серверному Web-приложению Консоль управления JMS из Web-браузера на клиентской машине добавьте в конфигурационный файл секцию "Kestrel" -> "Endpoints" -> "Https", например:

```

"Kestrel": {
  "Endpoints": {
    "Http": {
      "Url": "http://localhost:5001"
    },
    "Https": {
      "Url": "https://*:5000",
      "Certificate": {
        "Path": "<путь_к_pfx-файлу_сертификата>",
        "Password": "<пароль_к_pfx-файлу>"
      }
    }
  }
},

```

Где

- <путь\_к\_pfx-файлу\_SSL-сертификата> -- путь к файлу SSL-сертификата, выпущенного на имя хоста с серверным Web-приложением Консоль управления JMS;
- <пароль\_к\_pfx-файлу> - пароль к контейнеру сертификата;

Подробнее особенности синтаксиса прописывания адресов Kestrel (строковое значение параметра "Url") для JMS Web Admin приведены в разделе «Установка серверного компонента Консоли управления JMS», с. 20.

4. Для вступления в силу внесенных изменений перезапустите службу *eap-web-admin*:

```
systemctl restart eap-web-admin
```

### 17.3 Настройка SSL/TLS на стороне web-клиента JMS

Для корректного функционирования web-приложений с клиентом JMS или консолью управления JMS в конфигурационном файле JWA */etc/aladdin/jwa-service/appsettings.json* на клиентских компьютерах необходимо внести следующие изменения:

1. Для подключения по SSL к интерфейсу AuthenticationManager API (интерфейс аутентификации компонентов JMS) в секции "JMS", в параметре "AuthApiURL" впишите:

```
"JMS": {
  "AuthApiURL": "https://<FQDN_Сервера_JMS>:8121",
```

Где <FQDN\_Сервера\_JMS> -- полное доменное имя сервера JMS.

2. Для подключения по SSL к интерфейсу ClientManager API (интерфейс взаимодействия JMS с клиентскими компонентами – JWA) в секции "JMS", в параметре "ClientApiURL" впишите:

```
"JMS": {
  "ClientApiURL": "https://<FQDN_Сервера_JMS>:8122",
```

Где <FQDN\_Сервера\_JMS> -- полное доменное имя сервера JMS.

3. Для вступления в силу измененных параметров перезапустите процесс JWA командами:

```
/opt/jms-client/jwa-service.sh stop
/opt/jms-client/jwa-service.sh bg
```

## 17.4 Настройка SSL/TLS для работы с СУБД

### 17.4.1 Настройка SSL/TLS для работы с СУБД на стороне сервера JMS

Для включения поддержки защищённого соединения с СУБД при инициализации JMS (см. раздел «Установка и первоначальная настройка сервера и консольного агента JMS», с. 17) необходимо установить значение *true* у параметров:

- **encryptDatabaseConnection**
- **encryptServerConnection**

в секции **[database]** инициализационного файла (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS» с. 78).

### 17.4.2 Настройка SSL/TLS для работы с MS SQL

Настройка защищённого соединения для подключения к MS SQL выполняется через SQL Server Configuration Manager. Для настройки выполните следующие действия.

1. В разделе **Server Network Configuration** откройте контекстное меню, нажав правой кнопкой мышки на экземпляре сервера MS SQL, для которого производится настройка. В открывшемся меню выберите пункт **Properties**
2. В открывшемся диалоговом окне на вкладке **Flags** установите флаг **Force Encryption** в *Yes*, чтобы сделать SSL-подключения обязательными.

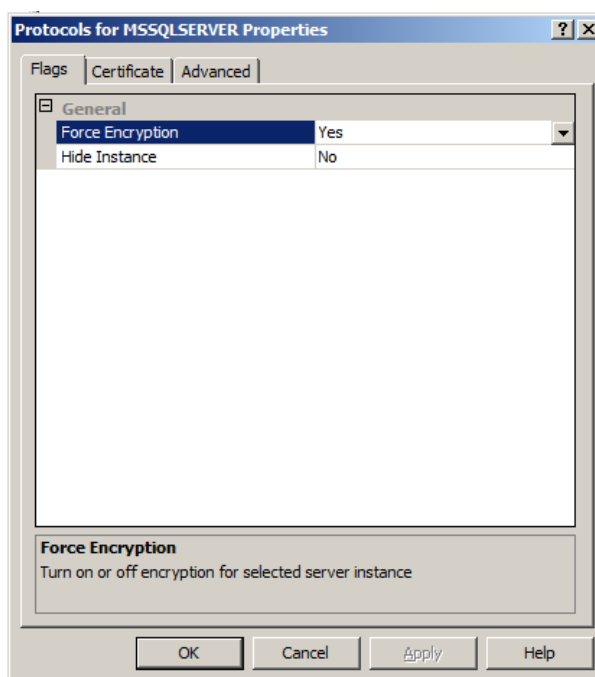


Рис. 53 – Установка принудительного включения защищённого соединения с MS SQL

3. На вкладке **Certificate** выберите сертификат, который будет использоваться для SSL-подключений.

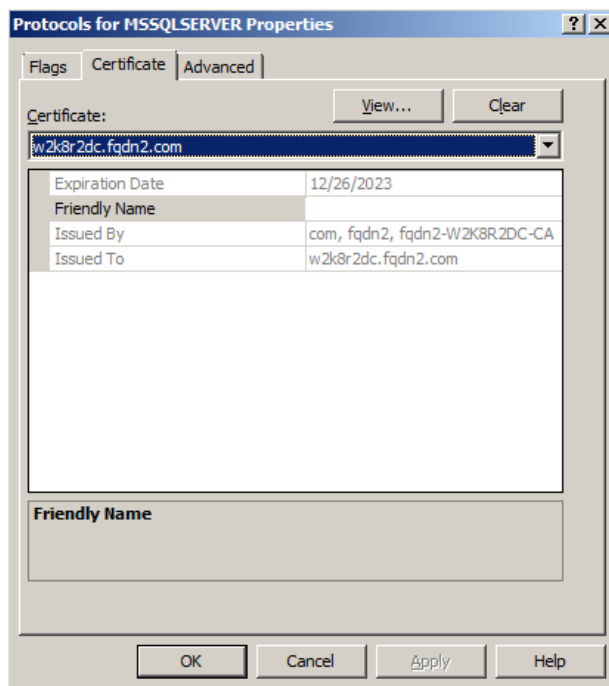


Рис. 54 – Выбор SSL-сертификата для защищённого соединения с MS SQL

- Если сертификат не выбран, то MS SQL создаст свой самоподписанный сертификат, что может быть нежелательным.
- Также необходимо отметить, что выбранный сертификат может не подойти под требования для SSL-сертификатов. В этом случае при запуске сервера MS SQL возникнет ошибка, связанная с SSL. Требования к сертификатам описаны документации к MS SQL: [Certificate requirements for SQL Server 2016](#)
4. Перезапустите экземпляр сервера MS SQL, для которого выполнялась настройка.

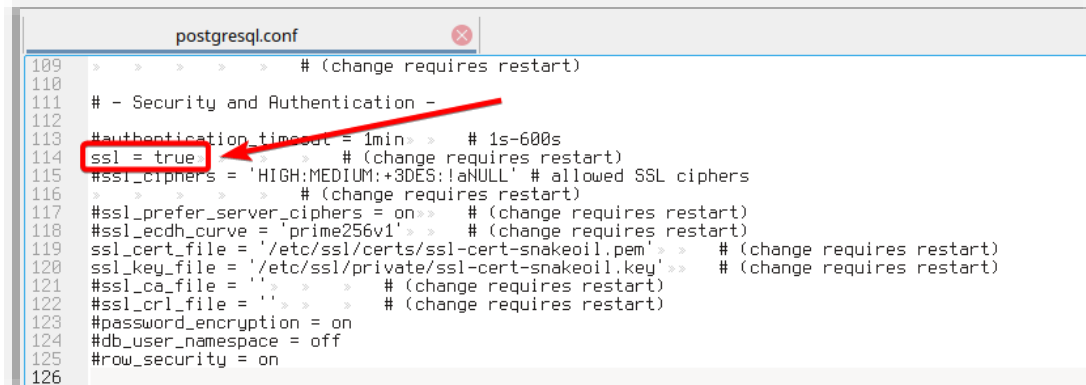
Более подробное описание настройки можно найти в документации к MSSQL. Например, для SQL Server 2016: <https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/configure-sql-server-encryption?view=sql-server-2016>.

#### 17.4.3 Настройка SSL/TLS для работы с PostgreSQL

После установки PostgreSQL обеспечивает опциональную (в зависимости от запросов клиента) поддержку SSL-соединений, но при этом используются временные (ssl-cert-snakeoil) сертификаты. Для обеспечения защищённого соединения с PostgreSQL, как правило, достаточно создать свои сертификаты и указать их в конфигурационном файле.

SSL для PostgreSQL настраивается в конфигурационном файле postgresql.conf. Для включения SSL выполните следующие действия.

1. Убедитесь, что у параметра `ssl` в конфигурационном файле установлено значение «true», «on» или «yes». Например в PostgreSQL версии 9.6 такой файл может выглядеть следующим образом:



```
109 >>>>> # (change requires restart)
110
111 # - Security and Authentication -
112
113 #authentication_timeout = 1min >> # 1s-600s
114 ssl = true <--
115 #ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers
116 >>>>> # (change requires restart)
117 #ssl_prefer_server_ciphers = on >> # (change requires restart)
118 #ssl_ecdh_curve = 'prime256v1' >> # (change requires restart)
119 ssl_cert_file = '/etc/ssl/certs/ssl-cert-snakeoil.pem' >> # (change requires restart)
120 ssl_key_file = '/etc/ssl/private/ssl-cert-snakeoil.key' >> # (change requires restart)
121 #ssl_ca_file = '' >> # (change requires restart)
122 #ssl_crl_file = '' >> # (change requires restart)
123 #password_encryption = on
124 #db_user_namespace = off
125 #row_security = on
126
```

Рис. 55 – Проверка включения режима SSL в конфигурационном файле PostgreSQL

2. Сгенерируйте ключевую пару, которая будет использоваться сервером PostgreSQL и укажите пути к файлу сертификата и ключа:

```
ssl_cert_file='/path/to/cert.pem'
ssl_key_file='/path/to/private/cert.key'
```

3. При необходимости укажите файлы со списком доверенных УЦ для клиентских сертификатов и списком отозванных сертификатов через параметры «`ssl_ca_file`» и «`ssl_crl_file`»:

```
ssl_ca_file=/path/to/root.crt
ssl_crl_file=/path/to/root.crl
```

4. Перезапустите PostgreSQL, если вносились какие-либо изменения в параметры выше:

```
sudo systemctl restart postgresql
```

Более детальное описание конфигурации SSL можно найти в документации PostgreSQL. Например, для версии 9.6 по следующей ссылке: <https://www.postgresql.org/docs/9.6/ssl-tcp.html>

## 17.5 Настройка SSL для доступа к ресурсной системе


Для обеспечения работы по SSL с ресурсной системой при инициализации сервера JMS необходимо установить значение `true` в параметре `useSsl` (в файле конфигурации, см. «Секция [accountSystem]», с. 79), а также убедиться в корректном значении порта (параметр `serverPort`).

Кроме того, для корректной работы с Samba AD или AD через SSL необходимо чтобы используемый серверный сертификат был доверенным и параметр `serverAddress` конфигурационного файла совпадал с CN сертификата или Subject Alternative Name.

В общем случае, если машина с сервером JMS не заведена в домен Samba AD или AD, следует выполнить следующий набор действий:

1. Добавить доменное имя машины с Samba AD в `/etc/hosts` серверной машины JMS.
2. Получить корневой сертификат ресурсной системы. Для Samba AD найти его можно командой «`sudo find / -name ca.pem`», обычно он находится в `/var/lib/samba/private/tls`. Для AD необходимо экспортировать корневой сертификат в формате «Base-64 encoded x.509»
3. После чего полученный сертификат необходимо сделать доверенным на машине с сервером JMS в соответствии с установленной на ней операционной системой:
  - Astra Linux
    - Убедиться, что установлен пакет `ca-certificates` (если нет, то поставить - "`apt-get install ca-certificates`")
    - Скопировать сертификат в `/usr/local/share/ca-certificates/`
    - Выполнить "`update-ca-certificates`"
  - РЕД ОС
    - Убедиться, что установлен пакет `ca-certificates` (если нет, то поставить - "`yum install ca-certificates`")
    - Выполнить "`update-ca-trust force-enable`"
    - Скопировать сертификат в `/etc/pki/ca-trust/source/anchors/`
    - Выполнить "`update-ca-trust extract`"
  - Alt Linux
    - Убедиться, что установлен пакет `ca-certificates` (если нет, то поставить - "`apt-get install ca-certificates`")
    - Скопировать сертификат в `/etc/pki/ca-trust/source/anchors/`
    - Выполнить "`update-ca-trust`"

Если же есть необходимость использовать Samba AD без SSL, то необходимо убедиться, что строка «`ldap server require strong auth = no`» присутствует в `/etc/samba/smb.conf`, если нет, то добавить её. Эта настройка отвечает за требование SSL со стороны Samba AD при подключении.

 **Примечание.** В случае если изначально сервер JMS был проинициализирован с отключенным флагом `useSsl` (`useSsl=false`, значение по умолчанию), можно произвести повторную инициализацию JMS, предварительно внося необходимые изменения в файл `InitialConfiguration.ini` (см. раздел «Подготовительные действия», с. 17). Кроме того, параметры подключения к ресурсной системе можно изменить с помощью графической утилиты JMS Web Console (Рис. 56).



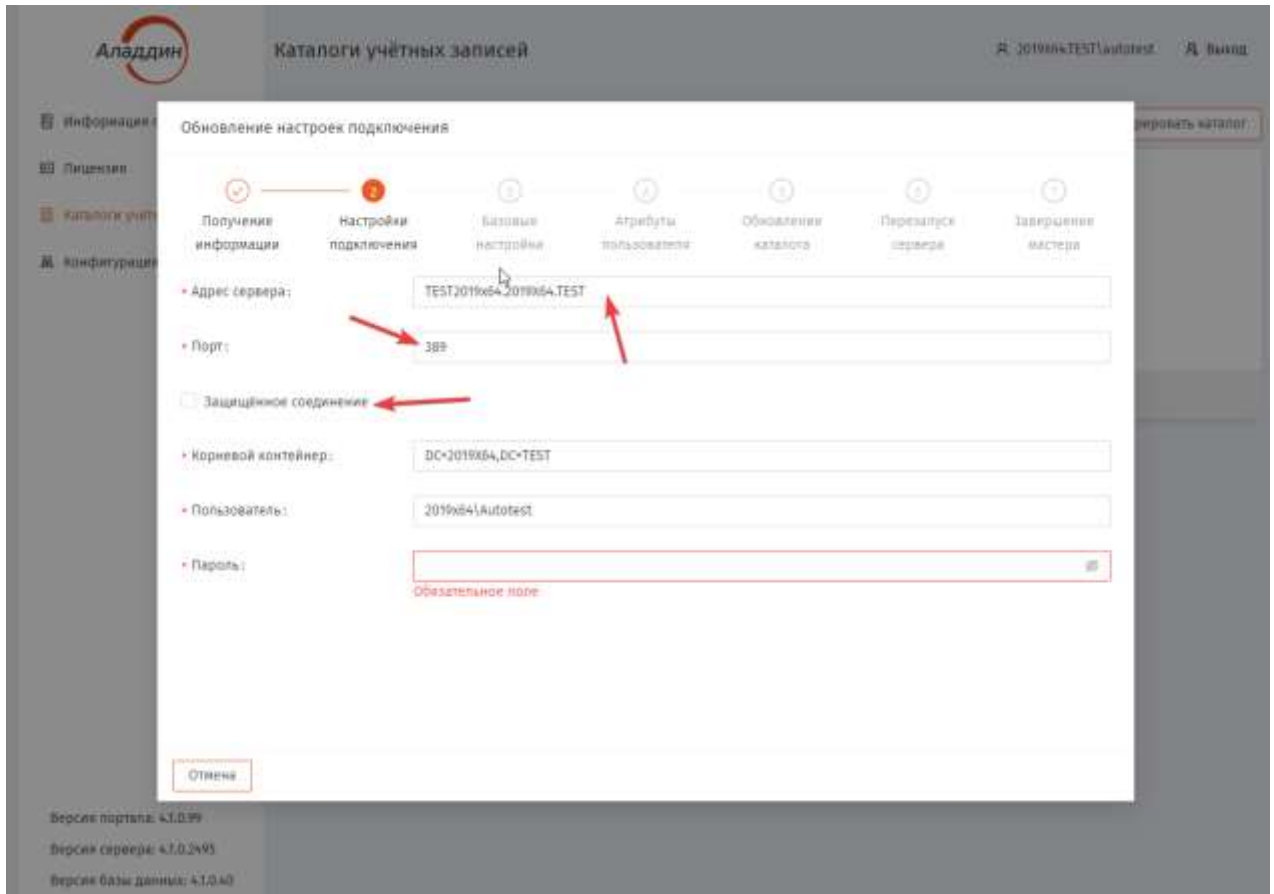


Рис. 56 – Изменение параметров подключения к ресурсной системе с помощью графической утилиты JMS Web Console

## 17.6 Настройка SSL в подсистеме JWM

Первоначальная настройка SSL в подсистеме JWM осуществляется с помощью файлов инициализации ее компонентов (подробнее см. раздел «Развёртывание JWM», с. 70). Однако если настройку SSL надо выполнить после инициализации компонентов JWM, выполните следующие шаги.

1. Выполните команду:

```
/opt/jms-web-manager/UserPlace/Configurator/ConfigureService userplace install cert
-path <path_to_pfx> --password <password_to_private_key>
```

где `-path` – путь до экспортированного сертификата в формате PFX  
`--password` – пароль от закрытого ключа

Например:

```
/opt/jms-web-manager/UserPlace/Configurator/ConfigureService userplace install cert
-path /opt/certs/jwmprivate.jms4.local.pfx --password P@ssw0rd!
```

2. Выполните команду:

```
/opt/jms-web-manager/UserPlace/Configurator/ConfigureService userplace install https  
-u URL:port
```

Например:

```
/opt/jms-web-manager/UserPlace/Configurator/ConfigureService userplace install https  
-u https://jwmpriate.jms4.local:5870
```

## 18. Порядок настройки прозрачной аутентификации доменных пользователей AD в клиентских приложениях JMS

В случае развёрнутой инфраструктуры Active Directory (AD) и включения в домен AD сервера JMS и клиентских компьютеров возможно настроить автоматическую аутентификацию доменных пользователей (по протоколу Kerberos) в JMS при использовании:

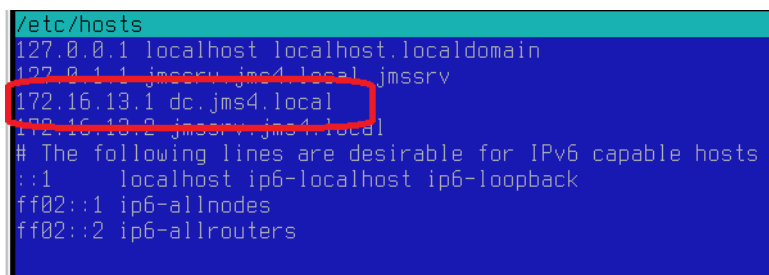
- web-приложения Консоль управления JMS;
- web-клиента JMS;
- приложения JWA tray.

Для настройки прозрачной аутентификации пользователей JMS на клиентских компьютерах выполните следующие действия.

1. Выполните генерацию файла *keytab* согласно разделу «Приложение 6. Порядок генерации файла *keytab* для прозрачной аутентификации в JMS пользователей из домена AD по протоколу Kerberos».
2. Полученный файл *keytab* (например *krb.keytab*) скопируйте на сервер JMS (например в папку */opt/conf*).
3. При конфигурировании файла *hosts* для IP-адреса контроллера домена укажите его DNS-имя:

```
<IP> DC.domain.name
```


Например:



```
/etc/hosts  
127.0.0.1 localhost localhost.localdomain  
127.0.1.1 jms4.local jms4.local jms4  
172.16.13.1 dc.jms4.local  
172.16.13.2 jms4.local jms4.local  
# The following lines are desirable for IPv6 capable hosts  
::1 localhost ip6-localhost ip6-loopback  
ff02::1 ip6-allnodes  
ff02::2 ip6-allrouters
```

Рис. 57 – Определение доменного имени сервера JMS в *hosts*

4. При инициализации сервера JMS (см. раздел «Установка и первоначальная настройка сервера и консольного агента JMS», с. 17) в его *ini*-файле следует выполнить следующие настройки:
  - адрес сервера ресурсной системы (т.е. контроллера домена AD см. параметр **serverAddress** в секции **[accountSystem]**) следует указать в формате полного DNS-имени (FQDN);
  - указать расположение файла *keytab* в параметре **keytabpath** секции **[service]**.

 **Примечание.** В случае если настройка прозрачной аутентификации осуществляется после инициализации сервера JMS, расположение файла *keytab* можно определить в конфигурационном файле *ear-engine/appsettings.json*, добавив секцию "KerberosTicketValidator":

```
{
  "Name": "KerberosTicketValidator",
  "Settings": {
    "KeyTablePath": "/opt/conf/krb.keytab"
  }
}
```

После переопределения файла следует перезапустить службу сервера JMS

5. На клиентских машинах отредактируйте конфигурационный файл JWA `/etc/aladdin/jwa-service/appsettings.json` таким образом, чтобы в адресах интерфейсов `IntegrationApiURL`, `AuthApiURL` и `ClientApiURL` адрес сервера JMS был представлен в формате FQDN, например:

```
"JMS": {
  "IntegrationApiURL": "http://jms4.local:8120",
  "AuthApiURL": "http://jms4.local:8121",
  "ClientApiURL": "http://jms4.local:8122"
},
```

6. Для прозрачной аутентификации в web-приложении Консоль управления JMS на стороне сервера JMS Web Admin в конфигурационном файле `/etc/aladdin/eap-web-admin/appsettings.json` отредактируете значение `"AuthenticationApiUrl"` таким образом, чтобы адрес сервера JMS был представлен в формате FQDN, например:

```
"WebAdminSettings": {
  ...
  "AuthenticationApiUrl": "http://jms4.local:8121"
```

7. Чтобы обеспечить корректную аутентификацию по протоколу Kerberos убедитесь, что на контроллере домена AD, сервере JMS и клиентских машинах системное время синхронизировано.
8. Для прозрачной аутентификации в web-браузере (подключение в web-клиенте JMS и в web-приложении Консоль управления JMS) на клиентском компьютере необходимо выполнить настройки автоматического запроса билета Kerberos в соответствии с документацией производителя соответствующего браузера.

Аутентификация в соответствующем web-приложении (в web-клиенте JMS или в web-приложении Консоль управления JMS) будет происходить автоматически, если сессия ОС была открыта от имени соответствующего доменного пользователя JMS (имеющего права доступа в соответствующем приложении JMS).

9. Для автоматической аутентификации доменного пользователя в JMS при открытии сессии в JWA Tray необходимо выполнить следующие настройки:
  - 9.1. Настроить конфигурационный файл JWA так, как это было сделано на шаге 5.
  - 9.2. Создать профиль **Настройка синхронизации рабочей станции** (см. руководство по функциям управления JMS [2], раздел «Профиль настройки синхронизации рабочей станции»), в котором необходимо установить флаг **Открывать сессию под текущей доменной учетной записью**, и привязать данный профиль к каталогу **Внедоменные рабочие станции**.

Аутентификация пользователя в приложении JWA tray будет происходить автоматически, если вход в ОС был осуществлен доменным пользователем, имеющим права доступа к JMS. Автоматическая регистрация JWA tray в JMS по протоколу Kerberos отображается специальным диалоговым окном:

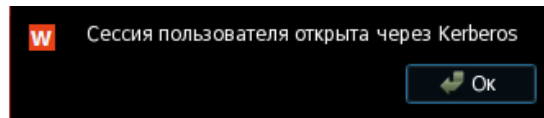



Рис. 58 – Оповещение об автоматическом открытии сессии через Kerberos

 **Примечание.** Для того чтобы проверить наличие билета Kerberos на клиентской машине можно воспользоваться командой `klist`.

## 19. Настройка внутренней точки доступа к IntegrationManager API

В текущей реализации JMS в технологических целях для обеспечения некоторых функций консольного агента ему предоставлен доступ через локальную (внутреннюю) точку доступа к сетевому интерфейсу IntergartionManager API (см. Рис. 50, с. 58). По умолчанию, используется адрес `http://localhost:8130`.


Если в целях безопасности необходимо отключить эту точку или изменить порт, следует отредактировать конфигурационный файл сервера `appsettings.json`. Для этого выполните следующие действия

1. Найдите блок настроек [`Name: IntegrationManagerWebApi`];
2. Создайте или измените параметр **EnableLocalhostEndpoint**, указав значение `false` (значение `true` означает состояние "включена", значение по умолчанию). Например:

```
{
  "Name": "IntegrationManagerWebApi",
  "Settings": {
    "IntegrationManagerWebApiAddresses": "http://*:8120",
    "EnableLocalhostEndpoint": "false",
  }
},
```

3. Создайте или измените параметр **LocalhostEndpointPort** чтобы изменить порт, на котором будет подниматься локальная точка доступа (значение по умолчанию: `8130`). Например:

```
{
  "Name": "IntegrationManagerWebApi",
  "Settings": {
    "IntegrationManagerWebApiAddresses": "http://*:8120",
    "LocalhostEndpointPort": "8140"
  }
},
```

 **Важно!** При отключении локальной точки доступа возможен отказ некоторых команд консольного агента, таких как `maintenance run`.

## 20. Компонент JMS Web Manager (JWM)

JMS Web Manager (JWM) – компонент JMS, предоставляющий возможность пользователям управлять через web-браузер своими OTP-аутентификаторами, а также электронными ключами, как внутри корпоративной сети, так и из-за её пределов через общедоступные сети.

JWM включает в себя следующие основные компоненты:

- **серверный компонент сервисов личного кабинета (ЛК)** – обеспечивает бизнес-логику работы ЛК и его взаимодействие с JMS и JAS. Может устанавливаться на отдельный сервер;
- **серверный компонент web-портала ЛК** – обеспечивает работу пользовательского web-интерфейса ЛК для удалённых пользователей, работающих через web-браузер. Портал ЛК может быть настроен для доступа пользователей как из внутренней корпоративной сети (private-режим), так и из внешней сети (public-режим). Каждый из порталов (внешний и внутренний) может устанавливаться на отдельный сервер.

Свои прикладные функции компонент JWM выполняет путем обращения к серверным компонентам JMS (JMS Server) и JAS (JaCarta Authentication Server) посредством соответствующих API-интерфейсов.

## 20.1 Дистрибутив

Табл. 13 – Установочные пакеты сервера JWM

ОС	Файл дистрибутива	Описание
Astra Linux	<b>aladdin-jwm-services_4.1.0.xxxx_x64.deb</b>	Установочные пакеты сервисов (Auth и Data) ЛК
РЕД ОС	<b>aladdin-jwm-services_4.1.0.xxxx_x64.rpm</b>	
ОС Альт	<b>aladdin-jwm-services_4.1.0.xxxx_alt_x64.rpm</b>	
Astra Linux	<b>aladdin-jwm-portal_4.1.0.xxxx_x64.deb</b>	Установочные пакеты портала ЛК
РЕД ОС	<b>aladdin-jwm-portal_4.1.0.xxxx_x64.rpm</b>	
ОС Альт	<b>aladdin-jwm-portal_4.1.0.xxxx_alt_x64.rpm</b>	

## 20.2 Системные требования компонентов JWM

Табл. 14 – Системные требования для установки компонентов JWM

Компонент среды функционирования	Требование
Операционная система	<ul style="list-style-type: none"> <li>• Astra Linux SE 1.7 Smolensk;</li> <li>• Astra Linux CE 2.13 Orel;</li> <li>• РЕД ОС 7.2, 7.3;</li> <li>• ОС Альт 8 СП</li> </ul>
Сервер СУБД	<ul style="list-style-type: none"> <li>• PostgreSQL версии 10;</li> <li>• Jatoba 1.9.1-3</li> </ul>
Дополнительное ПО	Пакеты, необходимые для работы .NET (см. инструкцию <a href="https://learn.microsoft.com/en-us/dotnet/core/install/linux-scripted-manual">https://learn.microsoft.com/en-us/dotnet/core/install/linux-scripted-manual</a> )

Компонент среды функционирования	Требование
Аппаратная платформа	Требования к аппаратной платформе совпадают с требованиями, предъявляемыми операционными системами, в которых развернуты серверные компоненты сервисов и web-портала ЛК (сервера JWM)
Оперативная память (не менее)	4 Гбайт
Свободное место на жестком диске (не менее)	1 Гбайт

### 20.3 Развёртывание JWM

Порядок установки JWM приводится на примере развёртывания типовой архитектуры, включающей в себя отдельные серверы для Auth- и Data-сервисов JWM, а также отдельные серверы для внешнего и внутреннего порталов JWM (Рис. 59).



**Примечание.** В примере развёртывания в качестве ресурсной системы приведена Microsoft Active Directory.

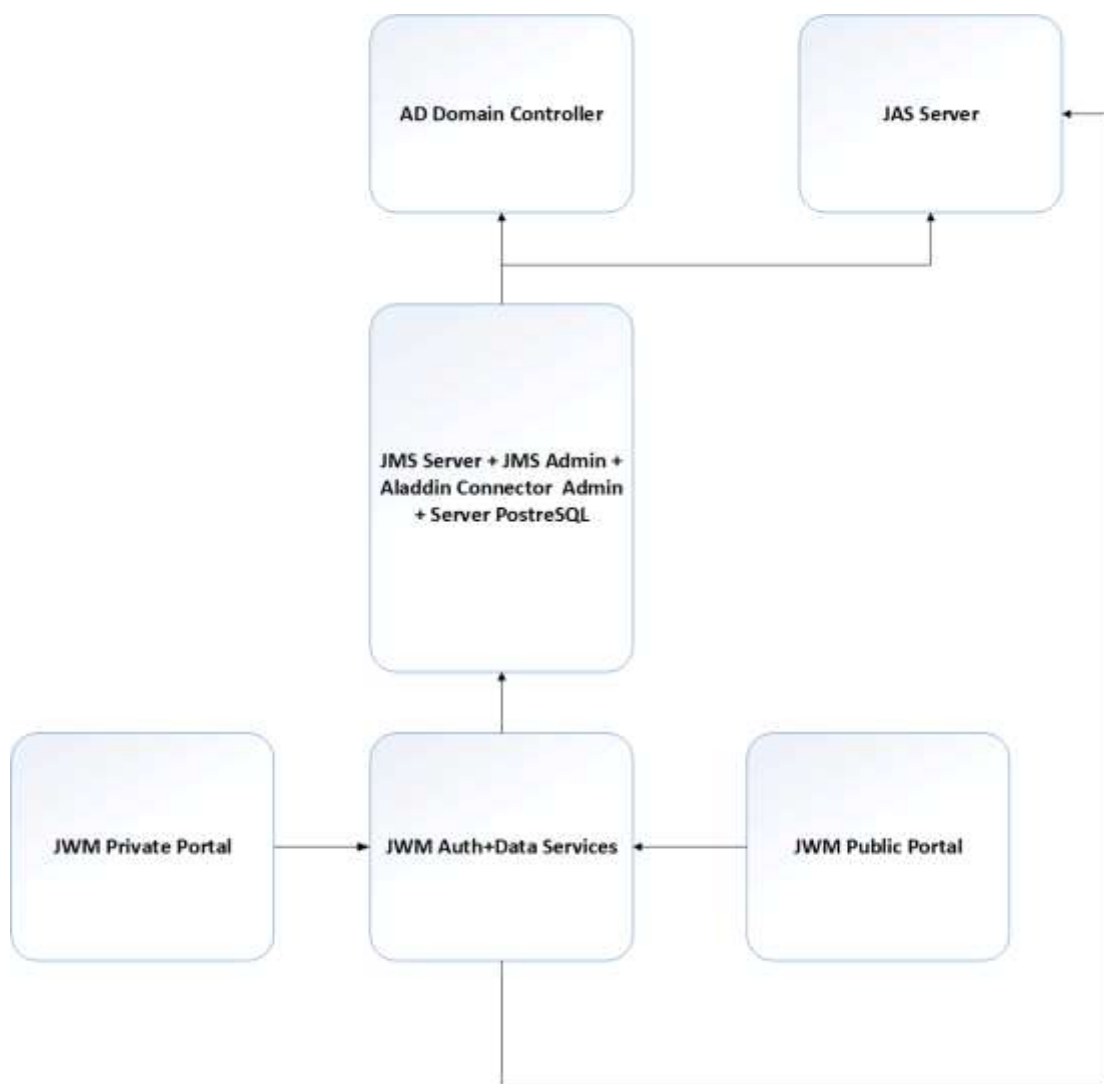


Рис. 59 – Пример типовой архитектуры развертывания JWM (описывается в разделе)

### 20.3.1 Подготовительные действия

Перед развертыванием JWM выполните следующие действия.

1. Для компьютеров, на которых будут установлены компоненты JWM, выпустите сертификаты в формате \*.pfx (экспорт сертификата следует выполнять с закрытым ключом). Данный сертификат используется для подписания JWT-токенов. При выпуске используются назначения «Проверка подлинности клиента», «Проверка подлинности сервера». При настройке компонента JMW данный pfx-файл следует указать в качестве параметра.



**Примечание.** В случае если выпущенный сертификат уже установлен на компьютер, при настройке соответствующего компонента JWM достаточно указать его отпечаток.

2. Убедитесь в сетевой связанности всех компьютеров для развёртывания компонентов JMW (по аналогии со схемой на Рис. 59, с. 71)

3. На каждый компьютер с компонентом JWM загрузите и отредактируйте ini-файл, содержащий информацию для инициализации устанавливаемого компонента.  
Пример такого файла приведен ниже:

```
;
; параметры порталов (фронтенд)
;

[userplace]
; адрес хостирования
url = https://*:5700
; сертификат для https
certificatePath = /home/admin/install/https/cert.pfx
certificatePassword = 1234567890
; Флаг отключающий проверку валидности сертификата по CRL и Root.
noValidate = true
; URL сервиса данных
dataUrl = http://jwm-services.devel.corp:5702
; таймаут обращения к сервису данных, в секундах
dataTimeout = 15
; использовать прокси для обращения к сервису данных
dataUseProxy = false
; адрес сервиса аутентификации и параметры соединения
authUrl = http://jwm-services.devel.corp:5703
; таймаут обращения к сервису аутентификации, в секундах
authTimeout = 15
; использовать прокси для обращения к сервису аутентификации
authUseProxy = false

[jwm]
; режим работы портала
; Public - внешний портал, Private - внутренний портал
mode = Private
; Виртуальный каталог
; совместно с адресом хостирования формирует URL для обращения
pathBase = /JMS/private

[cors]
; настройки CORS - если требуется обращение с другого сайта
endpoints = http://portal.devel.corp

; URL для поиска JMS Web Agent
[jwa]
http = http://localhost:5601
https = https://localhost:5600

;
; параметры сервисов (бэкенд)
;

[dataservice]
; адрес хостирования сервиса данных
url = http://*:5702
; сертификат для https
certificatePath =
certificatePassword =
; Флаг отключающий проверку валидности сертификата по CRL и Root.
noValidate = true

[authservice]
; адрес хостирования сервиса аутентификации
url = http://*:5703
; сертификат для https
certificatePath =
```



```
certificatePassword =
; Флаг отключающий проверку валидности сертификата по CRL и Root.
noValidate = true

[jms]
; адрес сервиса аутентификации JMS AuthenticationServiceWebApi
authApiUrl = http://jms.devel.corp:8121
; адрес сервиса администрирования JMS IntegrationManagerWebApi
clientApiUrl = http://jms.devel.corp:8120
; имя пользователя JMS для обращения к сервису администрирования
user = devel\admin
; пароль пользователя JMS для обращения к сервису администрирования
; указывается если сертификат JWT не совпадает с сертификатом STS
password =

[jas]
; URL сервиса аутентификации сервера JAS, если используется
url = http://jas.devel.corp:8221/api/v4.1

[database]
; тип СУБД
type=PostgreSQL
; адрес сервера СУБД
serverAddress=db-host.devel.corp
serverPort=5432
; серверный логин
serverLogin=postgres
serverPassword=12345678
; имя БД
databaseName=jwmdb
; пользователь БД
databaseLogin=postgres
databasePassword=12345678

;
; общая часть - параметры выпуска и проверки JWT
;

[jwt]
; с сертификатом на хосте сервисов (бэкенде) должен быть связан закрытый ключ
; если указать тот же сертификат, что используется JMS, пароль пользователя JMS
задавать не нужно

; файл сертификата для импорта, если сертификат не загружался ранее
certificatePath = /home/admin/install/jwt/cert.pfx
; пароль к файлу сертификата для импорта, если используется
certificatePassword = 0987654321
; Флаг отключающий проверку валидности сертификата по CRL и Root.
noValidate = true
; отпечаток ранее загруженного сертификата, если существует
thumbprint = 834E1F5B10ADB02BF54334AC0E60B82FDEB2E282
; время жизни токена в минутах, влияет на таймаут сессии пользователя
ttl = 15
; допуск времени при проверке JWT, в секундах
clockSkew = 60
```

Подробное толкование назначения секций и параметров ini-файла приведено в разделе «Приложение 7. Параметры файла первоначальной конфигурации компонентов сервера JWM», с. 108.

Файл инициализации можно разместить в произвольную директорию, которая будет указана в дальнейшем при конфигурировании соответствующего сервиса JWM.

### 20.3.2 Установка компонентов JWM

Порядок развёртывания компонентов JWM приведен на примере ОС Astra Linux.

1. Для установки сервиса внутреннего (Private) или внешнего (Public) порталов на соответствующий компьютер скопируйте дистрибутив согласно Табл. 13, с. 69 и выполните команду вида:

```
dpkg -i aladdin-jwm-portal_<version>_x64.deb
```

Например:

```
dpkg -i aladdin-jwm-portal_4.1.0.6226_x64.deb
```

2. Выполните перезагрузку демона следующей командой

```
systemctl restart jwm-portal.service
```

3. Для установки сервисов Auth и Data на соответствующий компьютер скопируйте дистрибутив согласно Табл. 13, с. 69 и выполните команду вида:

```
dpkg -i aladdin-jwm-services_<version>_x64.deb
```

Например:

```
dpkg -i aladdin-jwm-services_4.1.0.6226_x64.deb
```

4. Выполните перезагрузку демона следующей командой

```
systemctl restart jwm-services.service
```

### 20.3.3 Первоначальная настройка компонентов JWM

Для настройки сервисов Auth и Data выполните следующие действия.

1. На машине с установленными Auth- и Data-сервисами выполните их инициализацию с помощью следующей команды:

```
sudo /opt/jms-web-manager/DataService/Configurator/ConfigureService init -p  
<path_to_ini_file>
```

где <path\_to\_ini\_file> -- путь к ini-файлу, сформированному на подготовительном этапе.

Например:

```
sudo /opt/jms-web-manager/DataService/Configurator/ConfigureService init -p  
/opt/conf/jwm_initial_config.ini
```

Для настройки порталов (Private и/или Public) выполните следующие действия.

2. На машине с установленным порталом выполните его инициализацию с помощью следующей команды:

```
sudo /opt/jms-web-manager/UserPlace/Configurator/ConfigureService init -p  
<path_to_ini_file>
```

где <path\_to\_ini\_file> -- путь к ini-файлу, сформированному на подготовительном этапе.

Например:

```
sudo /opt/jms-web-manager/UserPlace/Configurator/ConfigureService init -p  
/opt/conf/jwm_initial_config.ini
```



**Примечание.** Если в домене не настроен список отзыва сертификатов (CRL), для корректной работы компонентов JWM, для которых в результате инициализации были установлены сертификаты для подписания JWT-токенов, на компьютерах, где установлены данные компоненты, можно установить необходимые флаги верификации сертификата командой:

```
sudo /opt/jms-web-manager/DataService/Configurator/ConfigureService jwt set cert_flags -v 4095 -t 15
```

Подробнее ознакомиться со всеми флагами верификации можно на web-ресурсе <https://learn.microsoft.com/ru-ru/dotnet/api/system.security.cryptography.x509certificates.x509verificationflags?view=net-7.0>

### 20.3.4 Подготовительные действия для самостоятельной установки JWA пользователями

Для того чтобы обеспечить возможность установки пользователями клиентского агента (JWA) на своих рабочих компьютерах по подсказке из web-клиента следует выполнить следующие действия.

После развертывания и настройки портала JWM в каталоге `/opt/jms-web-manager/UserPlace` следует создать вложенную папку следующего формата:

```
/wwwroot/modules/<платформа>
```

где вместо `<платформа>` - следует подставить "Win64", "Linux" или "MacOs" в зависимости от используемых клиентских операционных систем.

В каждый из созданных вложенных каталогов следует скопировать дистрибутив JWA для соответствующей платформы.

## 21. JWM-коннектор для JMS и консоли управления (JMS Web Admin)

JWM-коннектор для JMS представляет собой набор дополнительных компонентов для Сервера JMS и Консоли управления JMS, позволяющий управлять объектами JWM и правами пользователей по отношению к объектам JWM, доступным из личного кабинета пользователя.

JWM-коннектор включает в себя два компонента:

- модуль коннектора для сервера JMS, устанавливается на машину с компонентом JMS Server;
- модуль расширения для консоли управления JMS, устанавливается на машину с компонентом JMS Web Admin.

### 21.1 Дистрибутив

Табл. 15 – Установочные пакеты JWM-коннектора для JMS

ОС	Файл дистрибутива	Описание
Astra Linux	<b>aladdin-jwm-connector-server_4.1.0.xxxx_x64.deb</b>	Коннектор JWM, устанавливаемый на сервер JMS

ОС	Файл дистрибутива	Описание
РЕД ОС	<b>aladdin-jwm-connector-server_4.1.0.xxxx_x64.rpm</b>	Коннектор JWM, устанавливаемый на машину с JMS Web Admin
ОС Альт	<b>aladdin-jwm-connector-server_4.1.0.xxxx_alt_x64.rpm</b>	
Astra Linux	<b>aladdin-jwm-connector-admin_4.1.0.xxxx_x64.deb</b>	
РЕД ОС	<b>aladdin-jwm-connector-admin_4.1.0.xxxx_x64.rpm</b>	
ОС Альт	<b>aladdin-jwm-connector-admin_4.1.0.xxxx_alt_x64.rpm</b>	

## 21.2 Системные требования JWM-коннектора для JMS

Системные требования JWM-коннектора:

- для установки серверного компонента JWM-коннектор на сервере JMS необходимо обеспечить минимум 100 Мбайт дискового пространства, в остальном системные требования совпадают с системными требованиями к установке компонента JMS Server (см. раздел «Системные требования», с. 16);
- для установки компонента, предназначенного для консоли управления JMS, необходимо обеспечить минимум 100 Мбайт дискового пространства, в остальном системные требования совпадают с системными требованиями к установке компонента JMS Web Admin (см. раздел «Системные требования», с. 16).

## 21.3 Установка и настройка JWM-коннектора на серверах JMS и JMS Web Admin

Порядок установки компонентов JWM-коннектора приведен на примере ОС Astra Linux.

1. Для установки JWM-коннектора для сервера JMS скопируйте на сервер JMS дистрибутив согласно Табл. 15, с. 75 и выполните команду вида:

```
dpkg -i aladdin-jwm-connector-server_<version>_x64.deb
```

Например:

```
dpkg -i aladdin-jwm-connector-server_4.1.0.6226_x64.deb
```

2. Выполните команду *jwm initialize* консольного агента JMS:

```
Aladdin.EAP.Agent.Terminal jwm initialize
```

3. Выполните настройку коннектора для сервера JMS с помощью команды следующего вида:

```
sudo Aladdin.EAP.Agent.Terminal jwm configure --url <адрес DataService> -u <имя доменного пользователя в кавычках> -p <пароль_пользователя>
```

где <имя доменного пользователя в кавычках> – доменное имя пользователя (в формате "DOMAIN\username", в кавычках), которому в JMS назначена роль *Администратор ИБ*

Например:

```
sudo Aladdin.EAP.Agent.Terminal jwm configure --url  
http://jwmservices1.jms4.local:5702 -u "jms4\admin" -p P@ssw0rd
```



**Примечание.** Подробное описание команды *jwm configure* консольного агента JMS см. в разделе «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal», с. 83.

4. Для установки JWM-коннектора для JMS Web Admin скопируйте на сервер с приложением JMS Web Admin дистрибутив согласно Табл. 15, с. 75 и выполните команду вида:

```
dpkg -i aladdin-jwm-connector-admin_<version>_x64.deb
```

Например:

```
dpkg -i aladdin-jwm-connector-admin_4.1.0.6226_x64.deb
```

## Приложение 1. Параметры файла первоначальной конфигурации сервера JMS

### Секция [service]


Настройки сервиса JMS.

Имя настройки	Обязательность наличия	Описание
<b>execPath</b>	Да	Путь до исполняемого файла сервера JMS.
<b>integrationManagerUrls</b>	Нет	Адреса Admin WebAPI: административного API. Можно задать несколько адресов через «;». Для возможности использования API извне, один из адресов должен содержать внешний URL, либо с IP сервера, либо с его доменным именем. Например, « <a href="http://localhost:8120">http://localhost:8120</a> ; <a href="http://192.168.2.202:8120">http://192.168.2.202:8120</a> », если машина с сервером JMS имеет IP 192.168.2.202. Значение по умолчанию: <code>http://*:8120</code>
<b>controlManagerUrls</b>	Нет	Адреса Control WebAPI, используемого агентом сервера. Можно задать несколько адресов через «;». Значение по умолчанию: <code>http://localhost:8119</code>
<b>authenticationManagerUrls</b>	Нет	Адреса для Auth WebAPI: общей точки аутентификации для других API. Можно задать несколько адресов через «;». Значение по умолчанию: <code>http://*:8121</code>
<b>clientManagerUrls</b>	Нет	Адреса для Client WebAPI: клиентского API. Можно задать несколько адресов через «;». Значение по умолчанию: <code>http://*:8122</code>
<b>keytabpath</b>	Нет	Путь к KeyTab файлу для Kerberos-аутентификации.

### Секция [database]


Настройки базы данных JMS.

Имя настройки	Обязательность наличия	Описание
<b>type</b>	Да	Тип СУБД. Поддерживаемые значения: <ul style="list-style-type: none"> <li>• PostgreSQL</li> <li>• MSSQL</li> <li>• JatobaSQL</li> </ul>
<b>serverAddress</b>	Да	Адрес сервера БД
<b>serverPort</b>	Да	Порт сервера БД

<b>databaseName</b>	Да	Имя создаваемой БД
<b>databaseLogin</b>	Да	Имя пользователя, которое будет использоваться сервером JMS для доступа с создаваемой БД
<b>databasePassword</b>	Да	Пароль пользователя
<b>encryptDatabaseConnection</b>	Нет	<p>Указывает, необходимо ли использовать защищенное SSL-соединение для подключения сервера JMS к БД. Значение по умолчанию: <b>false</b></p> <p> <b>Примечание.</b> Для СУБД PostgreSQL и MSSQL значение <b>false</b> означает, что будет использоваться незащищенное соединение: в этом случае SSL-подключение будет устанавливаться, если того требуют настройки СУБД. Значение <b>true</b> делает установку безопасного подключения обязательным.</p>
<b>serverLogin</b>	Нет	<p>Имя пользователя-администратора, который будет использоваться мастером развертывания для создания БД. Если параметр не задан – будет использоваться режим развертывания без наличия административных прав, требующий предварительное создание пустой БД JMS при помощи скриптов.</p>
<b>serverPassword</b>	Нет	Пароль пользователя для мастера развертывания. Не используется в режиме развертывания без наличия административных прав на СУБД.
<b>encryptServerConnection</b>	Нет	<p>Указывает, необходимо ли использовать защищенное SSL-соединение при развертывании. Значение по умолчанию: <b>false</b></p>
<b>isCivic</b>	Нет	Флаг отвечающий за режим работы с КН SF/ГОСТ (по умолчанию "true", т.е. гражданский режим)

### Секция [accountSystem]

Настройки первичной ресурсной системы.

Имя настройки	Обязательность наличия	Описание
<b>type</b>	Да	<p>Тип ресурсной системы. В текущей версии поддерживаются только значения: «FreeIPA», «AD», «SambaAD»</p>
<b>name</b>	Нет	<p>Имя ресурсной системы, которое используется внутри JMS. Применяется для идентификации ресурсной системы, например, при аутентификации пользователя. По умолчанию – значение параметра «type».</p> <p> <b>Примечание.</b> Если в конфигурационном файле опущен параметр «name», то при аутентификации пользователя в качестве префикса (доменной части имени) следует указывать значение, заданное в параметре «type». Например, если type=FreeIPA, то в качестве логина пользователя admin следует указать «FreeIPA\admin». Если же параметр «name» указан явно (например «DirectoryAlias»), то в качестве доменной части имени пользователя следует указать это значение, например «DirectoryAlias\admin» Альтернативным способом аутентификации пользователя является указание в качестве доменного префикса</p> <ul style="list-style-type: none"> <li>• для <b>AD</b> и <b>SambaAD</b>: netbios-имени домена. Например для домена aladdin.local и пользователя admin допускается ввести значение aladdin\admin</li> <li>• для <b>FreeIPA</b>: полное (FQDN) имя домена. Например для домена astratest.local и пользователя admin допускается ввести значение astratest.local\admin</li> </ul>

Имя настройки	Обязательность наличия	Описание
<b>description</b>	Нет	Описание ресурсной системы, которое используется внутри JMS. По умолчанию – «».
<b>serverAddress</b>	Да	Адрес сервера ресурсной системы
<b>serverPort</b>	Да	Порт сервера ресурсной системы. При использовании Samba AD или AD с SSL порт сервера по умолчанию – 636, без SSL – 389. Для FreeIPA – 389.
<b>useSsl</b>	Нет	Определяет, будет ли использоваться SSL при подключении к ресурсной системе. На данный момент актуально только для Samba AD и AD. Подробнее см. в разделе «Настройка SSL для доступа к ресурсной системе», с. 63. По умолчанию – «false».
<b>container</b>	Да	Контейнер, который будет считаться корневым для ресурсной системы.
<b>userName</b>	Да	Имя пользователя, от имени которого сервер JMS осуществляет доступ к ресурсной системе. Для FreeIPA необходимо задавать полное Distinguished Name (DN) пользователя, например userName=uid=admin,cn=users,cn=accounts,dc=aladdin,dc=local Для AD и Samba AD необходимо задавать имя с префиксом в виде netBIOSName домена. Например для домена “fqdn5.com” и пользователя “Administrator” следует указать userName=FQDN5\Administrator
<b>password</b>	Да	Пароль пользователя.
<b>disabledContainers</b>	Нет	Список имён контейнеров ресурсной системы разделённых запятыми, которые должны быть проигнорированы JMS. Актуально для Samba AD. По умолчанию – «». Пример – «Program Data,System,Application».
<b>mapping</b>	Нет	Определяет, будет ли использоваться маппинг идентификаторов для контейнеров в PC (true/false). Актуально только при использовании FreeIPA. По умолчанию – «true».
<b>attributes</b>	Нет	Наименования регистрируемых атрибутов PC, перечисленные через запятую (к примеру, «sn,ou,givenName»). Для регистрации всех поддерживаемых атрибутов PC следует указать «*» По умолчанию – «*»
<b>referralChasing</b>	Нет	Настройка взаимодействия с ресурсными системами (LDAP и т.п.). Задаёт параметр EnableReferralChasing при подключении к ресурсной системе. Данная опция позволяет продолжить поиск в ресурсной системе и перенаправить клиента на другой сервер для получения результата в случае, если возвращается ссылка на объект. По умолчанию – «true».

## Секция [primaryUser]

Параметры создания первичного пользователя JMS.

Имя настройки	Обязательность наличия	Описание
<b>accountName</b>	Да	Имя аккаунта пользователя в первичной ресурсной системе. На основе этого аккаунта в JMS будет создан первый пользователь с административными правами.




### Секция [licenses]

Параметры поиска файлов лицензий JMS.

Имя настройки	Обязательность наличия	Описание
path	Да	Имя файла лицензии, включая полный путь к нему. Например. /opt/licenses/EAP.lic

### Секция [sts]

Параметры поиска сертификата для подписи JWT токенов.

Имя настройки	Обязательность наличия	Описание
certificateThumbprint	Да	Отпечаток, по которому будет производиться поиск сертификата для подписи JWT токенов. Поиск производится в хранилище CurrentUser\My.  <b>Примечание.</b> Если сертификат не используется (не зарегистрирован в ОС, см. раздел 5.1, с. 16), то параметр следует указать с пустым значением: <code>certificateThumbprint=</code>

### Секции [userProperty]

Секции userProperty (их может быть несколько) являются опциональными и позволяют задать набор дополнительных редактируемых атрибутов пользователей JMS.

Имя каждой секции должно содержать уникальный код атрибута и задаваться в формате [userProperty:<код\_атрибута>]. Например, чтобы добавить атрибут с кодом **jmsCustom1**, нужно добавить в файл следующую секцию:

```
[userProperty:jmsCustom1]
description=Custom Property #1
type=string
default=Default string value
minLength=0
maxLength=99
```

Имя настройки	Обязательность наличия	Описание
accountSystem	Нет	Имя ресурсной системы, в которую необходимо добавить атрибут. При отсутствии значения атрибут будет добавлен во все ресурсные системы, заданные в файле начальной конфигурации.
description	Нет	Описание атрибута. При отсутствии значения в качестве описания используется код атрибута.
type	Нет	Тип атрибута. Допустимые значения: <ul style="list-style-type: none"> <li>• <b>string</b> (значение по умолчанию)</li> <li>• <b>number</b></li> </ul>
default	Нет	Начальное значение атрибута

Имя настройки	Обязательность наличия	Описание
<b>minLength</b>	Нет	Минимальная количество символов в значении атрибута. Для типа <b>number</b> ограничивает количество цифр в значении.  Значение по умолчанию: <b>0</b>
<b>maxLength</b>	Нет	Максимальное количество символов в значении атрибута. Для типа <b>number</b> ограничивает количество цифр в значении.  Значение по умолчанию: <b>400</b>

## Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal

Синтаксис команды:

```
Aladdin.EAP.Agent.Terminal <команда> [[<параметр>] [<ключ>] [<аргумент>]] ...
[[<параметр>] [<ключ>] [<аргумент>]]
```

Для получения справки из консоли следует ввести следующую команду:

```
Aladdin.EAP.Agent.Terminal --help
```

Ключ --help работает на всех уровнях вложенности команд консольного агента (т.е. его можно использовать также после *команды* или *параметра*), например

```
Aladdin.EAP.Agent.Terminal certificates install --help
```

Ниже приведен полный перечень *команд*, *параметров* и *ключей* консольного агента.

### Команда a2fa

Настройка подключения к серверу Aladdin 2FA

Параметр	Описание
<b>show</b>	<p>Отображает текущие настройки подключения к серверу Aladdin 2FA и также статус подключения.</p> <p><b>Пример выдачи:</b></p> <pre>(root@onkyu92-jm1) jms-service# echo /opt/eap-engine/eap-agent/aladdin.EAP.Agent.Terminal a2fa show Использовать сервер Aladdin 2FA: Да Адрес сервера: https://192.150.100.121:9000 Валидировать сертификат: Нет Статус подключения к Aladdin 2FA: Подключено</pre>
<b>configure</b>	<p>Выполняет настройку подключения к Aladdin 2FA.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-u, --url</b> (обязательный) -- адрес сервера Aladdin 2FA;</li> <li>• <b>-v, --validate</b> (опциональный) – проверять сертификат при подключении к Aladdin 2FA (допустимые значения: <b>False, True</b>)</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal a2fa configure -u https://192.150.100.121:9000 -v False</pre>
<b>enable</b>	<p>Включить использование сервиса Aladdin 2FA:</p> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal a2fa enable</pre>
<b>disable</b>	<p>Отключить использование сервиса Aladdin 2FA:</p> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal a2fa disable</pre>

## Команда accountsystem




## Регистрация и обновление ресурсной системы

Параметр	Описание
<b>list</b>	<p>Отображает список зарегистрированных ресурсных систем.</p> <p><b>Примеры выдачи:</b></p> <pre>root@lx-jms4:~# Aladdin.EAP.Agent.Terminal accountsystem list 1. Тип: FreeIPA      Имя: astratest.localNetBios: astratest.local  root@freeipa-orel:/home/autotest# eap-agent accountsystem list 1. Тип: FreeIPA      Имя: FreeIPA      NetBios: fqdn3.com 2. Тип: AD/Samba AD  Имя: ad321        NetBios: 2019X64</pre>
<b>register</b>	<p>Позволяет зарегистрировать новую ресурсную систему.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-p, --path</b> (обязательный) – путь (включая имя файла) к файлу конфигурации ресурсной системы</li> </ul> <p><b>⚠️ Важно!</b> После регистрации новой ресурсной системы необходимо перезапустить службу серверного компонента web-приложения Консоль управления JMS (пример команды см. в разделе «Установка серверного компонента Консоли управления JMS», с. 20) для ее корректной работы.</p> <p><b>📄 Примечание.</b> В качестве файла конфигурации ресурсной системы следует использовать файл в формате файла первоначальной конфигурации, содержащий секцию [accountSystem] (образец файла приведен в разделе «Установка и первоначальная настройка сервера и консольного агента JMS», с. 17. Описание параметров секции [accountSystem] файла приведено в разделе «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», «Секция [accountSystem]», с. 79)</p> <p>Для регистрации ресурсной системы требуется файл конфигурации с секцией «[accountSystem]», аналогичный файлу первоначальной конфигурации. Поддерживается регистрация сразу нескольких ресурсных систем. Для этого необходимо добавить дополнительные секции в зависимости от количества ресурсных систем «[accountSystem2]», «[accountSystem3]» и т.д.</p>
<b>update</b>	<p>Позволяет обновить информацию о зарегистрированной ресурсной системы.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-p, --path</b> (обязательный) – путь (включая имя файла) к файлу конфигурации ресурсной системы</li> <li>• <b>--accountsystem</b> (обязательный) – имя ресурсной системы указанное в поле [accountSystem] -&gt; name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», «Секция [accountSystem]», с. 79)</li> </ul> <p><b>📄 Примечание.</b> В качестве файла конфигурации ресурсной системы следует использовать файл в формате файла первоначальной конфигурации, содержащий секцию [accountSystem]</p> <p>Для обновление информации о ресурсной системе требуется файл конфигурации с секцией «[accountSystem]», аналогичный файлу первоначальной конфигурации. Поддерживается обновление сразу нескольких ресурсных систем. Для этого необходимо добавить дополнительные секции в зависимости от количества ресурсных систем «[accountSystem2]», «[accountSystem3]» и т.д.</p> <p>По умолчанию сопоставление конфигурации и ресурсной системы, для которой она предназначена, производится по имени (параметр name раздела «[accountSystem]»). При необходимости переименовать ресурсную систему в JMS в секции «[accountSystem]» необходимо в качестве name задать новое название, а в качестве oldName – текущее.</p>

Параметр	Описание
----------	----------

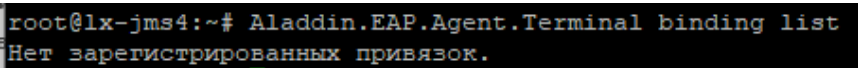
### Команда applet

Настройка поддерживаемых приложений в ЭК; влияет на число типов профилей инициализации ЭК, отображаемых в Консоли управления JMS

Параметр	Описание
<b>show</b>	<p>Табличное отображение включённых приложений (апплетов), для отображения соответствующих профилей в Консоли управления JMS.</p> <p><b>Пример выдачи команды на терминале:</b></p>  <p>Числовой идентификатор приложения (апплета) отображается слева.</p> <p>Звездочкой [*] отображается включенное приложение.</p>
<b>enable</b>	<p>Включить приложения (апплеты) с указанными числовыми идентификаторами. Для получения идентификаторов приложений следует выполнить команду с параметром Show (выше). Идентификаторы перечисляются через пробел, например:</p> <pre>Aladdin.EAP.Agent.Terminal applet enable 3 4</pre> <p>Для включения всех приложений в качестве идентификатора следует указать <i>all</i>, например:</p> <pre>Aladdin.EAP.Agent.Terminal applet enable all</pre> <p> <b>Примечание.</b> После включения приложений происходит автоматическая перезагрузка сервера JMS.</p>
<b>disable</b>	<p>Отключить приложения (апплеты) с указанными числовыми идентификаторами. Синтаксис команды аналогичен синтаксису команды с параметром <b>enable</b> (выше).</p> <p> <b>Примечание.</b> После отключения приложений происходит автоматическая перезагрузка сервера JMS.</p>

### Команда binding

Управление привязкой ресурсных систем

Параметр	Описание
<b>list</b>	<p>Отображает список зарегистрированных привязок.</p> <p><b>Пример выдачи:</b></p> 

Параметр	Описание
<b>add</b>	<p>Позволяет добавить новую привязку ресурсных систем.</p> <p>Процесс привязки происходит в интерактивном режиме:</p> <ol style="list-style-type: none"> <li>1. Выбор основной ресурсной системы из списка</li> <li>2. Выбор атрибута для привязки из основной ресурсной системы</li> <li>3. Выбор зависимой ресурсной системы из списка</li> <li>4. Выбор атрибута для привязки из зависимой ресурсной системы</li> </ol>
<b>update</b>	<p>Позволяет добавить новую ресурсную систему в существующую привязку.</p> <p>Процесс привязки происходит в интерактивном режиме:</p> <ol style="list-style-type: none"> <li>1. Выбор существующей привязки</li> <li>2. Выбор зависимой ресурсной системы из списка</li> <li>3. Выбор атрибута для привязки из зависимой ресурсной системы</li> </ol>

### Команда certificates

Управление сертификатами, используемыми в подсистеме аутентификации JMS, т.е. для подписи JWT-токенов

Параметр	Описание
<b>list</b>	<p>Выводит краткую информацию о сертификатах в хранилище CurrentUser\My</p> <p><b>Пример выдачи:</b></p> <pre>autotest@astra:~\$ sudo Aladdin.EAP.Agent.Terminal certificates list Listing certificate from 'My' certificate store (location: CurrentUser).       Thumbprint: C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2      Name:      SN: CN Done.</pre>
<b>install</b>	<p>Устанавливает сертификат в хранилище CurrentUser\My.</p> <p>В качестве входных параметров (ключи --path и --password) передается pfx-файл контейнера сертификата с закрытым ключом и его пароль.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>--path</b> (обязательный) – имя pfx-файла с его путем в файловой системе;</li> <li>• <b>--password</b> (обязательный) – пароль pfx-файла.</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal certificates install --path /mnt/hgfs/SmolenskShared/example.pfx --password 123456</pre>
<b>remove</b>	<p>Удаляет сертификат с указанным отпечатком из хранилища CurrentUser\My. Отпечаток можно получить в результате выполнения команды с параметром <b>list</b>.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-t</b> (обязательный) – отпечаток сертификата в шестнадцатеричном формате (см. Выдачу команды с параметром <b>list</b>);</li> </ul>

Параметр	Описание
	<p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal certificates remove -t C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2</pre>

## Команда connector

Отображение списка коннекторов

Параметр	Описание
<b>show</b>	<p>Команда позволяет отобразить список зарегистрированных коннекторов для синхронизации и список зарегистрированных адаптеров для коннектора к УЦ.</p> <p><b>Пример выдачи:</b></p> <pre>Зарегистрированные коннекторы: Имя Описание Лицензия 1. Коннектор для работы с УЦ Коннектор поддерживает выполнение действий над сертификатами: выпуск, отзыв, приостановление действия, возобновление действия Есть  Зарегистрированные адаптеры: Имя Описание 1. MsCertificateAuthority Адаптер для работы с Microsoft CA 2. DogtagCertificateAuthority Dogtag CA Adapter</pre>

## Команда cryptodb

Команда взаимодействия с СКЗИ КриптоБД

Параметр	Описание
<b>status</b>	<p>Отображает текущий статус подключения к КриптоБД</p> <p><b>Пример выдачи:</b></p> <pre>autotest@freeipa-ora1 ~\$ Aladdin.EAP.Agent.Terminal cryptodb status Текущее состояние КриптоБД: Подключен (Сервер ключей КриптоБД запущен. Работа JMS с авторизованными данными разрешена). autotest@freeipa-ora1 ~\$</pre>
<b>config</b>	<p>Выполняет выгрузку информации о текущей инсталляции JMS для последующего импорта в Консоль конфигурирования КриптоБД с целью настройки шифрования БД.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>-p, --path – путь к xml-файлу с конфигурацией КриптоБД (обязательный параметр)</li> <li>-l, --login – имя пользователя БД Postgres, используемый JMS при работе с КриптоБД (опциональный). Если не указан, то используется текущий логин JMS</li> <li>-m, --mask – маска (10 Байт) для отображения зашифрованных данных (при доступе неавторизованных пользователей). В текущей версии продукта указанное в команде значение игнорируется и подставляется значение 0000000000.</li> </ul> <p><b>Пример выдачи:</b></p> <pre>autotest@freeipa-ora1 ~\$ Aladdin.EAP.Agent.Terminal cryptodb config --path /tmp/EAP0B.xml Конфигурация КриптоБД выгружена в файл: /tmp/EAP0B.xml autotest@freeipa-ora1 ~\$</pre>


## Команда jas

### Настройка подключения к серверу JAS

Параметр	Описание
<b>show</b>	<p>Отображает текущие настройки подключения к серверу JAS (адрес и параметру аутентификации), а также статус подключения.</p> <p><b>Пример выдачи:</b></p> <pre>PS D:\ITA\Aladdin\earcore\OUTPUT\Bin\Debug\AnyCPU&gt; .\Aladdin.EAP.Agent.Terminal.exe jas show Адрес сервера JAS: http://localhost:8228 Способ аутентификации: Basic Логин к JAS: JAS\azatic_net Статус подключения к JAS: Подключено</pre>
<b>configure</b>	<p>Выполняет настройку подключения к JAS.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-u, --url</b> (обязательный) – адрес сервера JAS;</li> <li>• <b>-s, --securityType</b> – способ аутентификации при подключении к JAS (<b>None, Basic, Windows</b> или <b>NTLM</b>), значение по умолчанию: <b>None</b></li> <li>• <b>-l, --login</b> – Логин к JAS.</li> <li>• <b>-p, --password</b> – Пароль к JAS.</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal jas configure -u http://localhost:8220 -s Basic -l DOMAIN\jas -p zxasqw12!@</pre>

## Команда jwm

### Настройка подключения к JWM

 **Важно!** Команда доступна только после установки JWM-коннектора для JMS, см. раздел «JWM-коннектор для JMS и консоли управления (JMS Web Admin)», с. 75

Параметр	Описание
<b>configure</b>	<p>Команда выполняет настройку подключения сервера JMS к сервису данных JWM.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>--url</b> (обязательный) – адрес сервиса данных JWM;</li> <li>• <b>-u</b> – доменное имя пользователя (в формате "DOMAIN\username", в кавычках), которому в JMS назначена роль Администратор ИБ. От имени данного пользователя будет запускаться план обслуживания JWM</li> <li>• <b>-p</b> – Пароль пользователя, указанного в параметре -u</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal jwm configure --url http://jwmservices1.jms4.local:5702 -u "jms4\admin" -p P@ssw0rd!</pre>



Параметр	Описание
<b>initialize</b>	<p>Команда выполняет подключение сервера JMS к сервису данных JWM.</p> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal jwm configure initialize</pre>

## Команда jwt



Управление параметрами подписи JWT-токенов

Параметр	Описание
<b>show</b>	<p>Отображает текущие настройки подписи JWT-токенов. Не требует ключей.</p> <p><b>Пример выдачи:</b></p> <pre>autotest@astra:~\$ sudo Aladdin.EAP.Agent.Terminal jwt show Use certificate: False Thumbprint: C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2</pre>
<b>configure</b>	<p>Задаёт настройки подписи JWT-токенов.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>--useCertificate</b> (опциональный) – флаг необходимости использования сертификата для подписи JWT-токенов;</li> <li>• <b>-t</b> (опциональный) – отпечаток сертификата в шестнадцатеричном формате (см. Выдачу команды с параметром <b>list</b>);</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal jwt configure --useCertificate true -t C7B7C9E133BF5D194CCF7F027FF301DC3F9068D2</pre> <p>– включение использования подписи JWT-токенов ассиметричным ключом с указанием соответствующего сертификата</p> <pre>Aladdin.EAP.Agent.Terminal jwt configure --useCertificate false</pre> <p>– включение использования подписи JWT-токенов так называемым «симметричным ключом» (symmetric signing of JWT).</p>

## Команда licenses

Управление лицензиями JMS


Параметр	Описание
<b>list</b>	<p>Выводит информацию о текущих зарегистрированных лицензиях.</p> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal licenses list</pre>




Параметр	Описание
	<p><b>Фрагмент выдачи:</b></p> <pre>autotest@astra:~\$ sudo Aladdin.EAP.Agent.Terminal Id: 1 Comment: Purpose: ProductId: 0x0811 ProductName: Enterprise Application Platform</pre> <p>Значение параметра «Id» (внутренний идентификатор лицензии) может быть использовано в команде <code>remove</code> для удаления.</p>
<p><b>register</b></p>	<p>Регистрирует лицензию в JMS.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-p</b> (обязательный) – имя файла лицензии (.lic) с его путем в файловой системе;</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal licenses register -p /mnt/hgfs/SmolenskShared/Licenses/EAP.lic</pre> <p> <b>Примечание.</b> Перед регистрацией новой лицензии следует удалить ранее зарегистрированную (см. команду <code>licenses remove</code>)</p>
<p><b>remove</b></p>	<p>Удаляет лицензию из JMS. В качестве аргумента принимает внутренний идентификатор лицензии (можно получить с помощью команды <code>list</code>).</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-i</b> (обязательный) – внутренний идентификатор лицензии (можно получить с помощью команды с параметром <code>list</code>).</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal licenses remove -i 1</pre>
<p><b>replace</b></p>	<p>Заменяет существующую лицензию в JMS на новую.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-p</b> (обязательный) – полный путь к файлу лицензии (включая имя файла)</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal licenses replace -p /mnt/hgfs/SmolenskShared/Licenses/EAP.lic</pre> <p> <b>Примечание.</b> Команда требует ввода:</p> <ul style="list-style-type: none"> <li>• логина пользователя с ролью Оператор в формате:  <code>&lt;имя_ресурсной_системы&gt;\&lt;имя_пользователя&gt;</code>,</li> </ul> <p>где <code>&lt;имя_ресурсной_системы&gt;</code> – значение, указанное в поле <code>[accountSystem] -&gt; name</code> файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78)</p> <ul style="list-style-type: none"> <li>• и его пароля</li> </ul>
<p><b>request</b></p>	<p>Генерирует запрос на активацию продукта в формате PDF. В качестве аргументов принимает контактную информацию (название компании, ответственное лицо, должность, e-mail, контактный телефон), дату начала действие постоянной лицензии и имя файла запроса, который будет сгенерирован.</p>

Параметр	Описание
	<p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>-o (обязательный) – полный путь к формируемому файлу запроса (включая имя)</li> <li>-c (обязательный) – название компании</li> <li>-f (обязательный) – ФИО ответственного лица</li> <li>-t (обязательный) – Должность ответственного лица</li> <li>-e (обязательный) – адрес электронной почты ответственного лица</li> <li>-p (обязательный) – телефон ответственного лица</li> <li>-d (обязательный) – дата начала действия постоянной лицензии</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal licenses request \ -o /home/autotest/JMS_Activation_request.pdf \ -c "Horns&amp;Hooves" \ -f "Ivan Petrov" \ -t Manager \ -e test@test.com \ -p +79991234567 \ -d 03.05.2021</pre>

## Команда maintenance

### Управление планами обслуживания

Параметр	Описание
list	<p>Производит отображение всех доступных планов обслуживания, их описания, GUID и списка параметров (см. ключ -p для команды <b>maintenance run</b>, ниже )</p> <p><b>Пример выдачи:</b></p> <pre>admin@lx-jms4:~\$ Aladdin.EAP.Agent.Terminal maintenance list - 'План обслуживания ключевых носителей', GUID '4578a30a-e423-f2ef-b235-75e564b8b679' - 'Отзыв/отключение ключевого носителя в случае удаления или блокировки пользователя.' - 'Проверка привязки назначенных ключевых носителей к контейнеру.' - 'Проверка привязки неназначенных ключевых носителей к контейнеру.' - 'Проверка на наличие свободных ключевых носителей меньше порогового значения.' - 'MinRegisteredTokensCount' (10), 'Порог минимального количества свободных ключевых носителей'</pre>
run	<p>Производит добавление плана обслуживания в очередь выполнения.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>-g, --guid (обязательный) – GUID идентификатор плана обслуживания</li> <li>-p, --parameters (опциональный) – параметры для указанного плана обслуживания. Параметры могут перечисляться через пробел и указываются в формате "param1=value1" "param2=value2" ... "paramN=valueN"</li> </ul> <p> <b>Примечания:</b></p> <ol style="list-style-type: none"> <li>В случае если в строке отдельного параметра (для ключа -p) отсутствуют пробелы допускается его указание без кавычек, например <i>param1=value1</i></li> <li>При пропуске опционального ключа -p будут использованы параметры из БД JMS, т.е. их значения на момент последней настройки соответствующего плана обслуживания через консоль управления JMS. Если из консоли управления JMS изменений плана не проводилось, то будут использованы значения, установленные по умолчанию при развёртывании сервера JMS. <b>Для гарантирования устойчивости выполнения планов обслуживания JMS рекомендуется значение ключа -p всегда указывать явно.</b></li> </ol>


Параметр	Описание
	<p><b>Примеры команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal maintenance run -g 78960243-7a21-62aa-a02b-73622a5f39b1 -p "AccountSystemName=fqdn2.com" "ParentObjectId="</pre> <pre>Aladdin.EAP.Agent.Terminal maintenance run -g 78960243-7a21-62aa-a02b-73622a5f39b1 -p "AccountSystemName=fqdn2.com" ParentObjectId=</pre> <p><b>Пример выдачи:</b></p>  <p><b>Примечания:</b></p> <ol style="list-style-type: none"> <li>1) Для получения готовой команды <b>maintenance run</b> (со всеми параметрами, включая GUID-идентификаторы контейнеров ресурсной систем и самого плана обслуживания) можно воспользоваться сервисом автоматической генерации команды (см. раздел «Автоматическая генерация параметров запуска команды maintenance run», с. 46)</li> <li>2) Для получения полного списка GUID-идентификаторов, и параметров для ключа <b>-p</b> воспользуйтесь командой <b>maintenance list</b> (см. выше).</li> <li>3) Подробное описание назначения параметров запуска для каждого из планов обслуживания приведено во второй части руководства администратора [2], в разделе «Планы обслуживания».</li> <li>4) JMS позволяет организовывать очереди из заданий на выполнение планов обслуживания, подробнее см. «Автоматическая организация очередей выполнения заданий планов обслуживания», с. 44</li> </ol>
<b>cancel</b>	<p>Производит отмену выполнения ранее добавленного в очередь плана обслуживания.</p> <p><b>Ключ:</b></p> <p><b>-g, --guid</b> (обязательный) – GUID идентификатор плана обслуживания.</p> <p><b>Пример выдачи:</b></p> 
<b>status</b>	<p>Производит получение текущего состояния плана обслуживания.</p> <p><b>Ключ:</b></p> <p><b>-g, --guid</b> (обязательный) – GUID идентификатор плана обслуживания.</p> <p><b>Пример выдачи:</b></p> 

## Команда server

### Управление сервером JMS

Параметр	Описание
<b>status</b>	Вывод текущего статуса сервера. (Не требует ключей.)
<ul style="list-style-type: none"> <li>• <b>start</b></li> <li>• <b>stop</b></li> <li>• <b>pause</b></li> <li>• <b>continue</b></li> </ul>	<p>Управление статусом сервера. (Не требует ключей.)</p> <ul style="list-style-type: none"> <li>• <b>start</b> – запуск сервера</li> <li>• <b>stop</b> – остановка сервера</li> </ul>


Параметр	Описание
	<ul style="list-style-type: none"> <li>• <b>pause</b> – приостановление работы сервера</li> <li>• <b>continue</b> – восстановить работу сервера после установки на паузу</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal server stop</pre>
<p><b>initialize</b></p>	<p>Инициализирует сервер JMS: выполняет последовательную настройку всех параметров конфигурации сервера JMS, определенную в ini-файле конфигурации (передается в параметре ключа -p). Пример ini-файла см. в разделе «Подготовительные действия», с. 17.</p> <p><b>⚠ Важно!</b> Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>-p</b> (обязательный) – файл (.ini) конфигурации сервера JMS вместе с путём в файловой системе;</li> <li>• <b>-t</b> (опциональный) -- значение таймута для операций запуска/остановки сервера в миллисекундах;</li> <li>• <b>--password</b> (опциональный) -- пароль, значение которого должно соответствовать паролю пользователя accoputName, указанному в ini-файле первоначальной конфигурации сервера JMS в секции [primaryUser] (см. раздел «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78). Если параметр будет пропущен, то консольный агент запросит пароль в процессе инициализации сервера.</li> </ul> <p><b>Пример команды:</b></p> <pre>sudo Aladdin.EAP.Agent.Terminal server initialize -p /mnt/hgfs/SmolenskShared/conf.ini -t 120000</pre>
<p><b>update</b></p>	<p><b>⚠ Важно!</b> Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo.</p> <p>Выполняет проверку на необходимость обновления базы данных, и если требуется обновление, предлагает его выполнить.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>--allowautoupdate</b> – при указании параметра, в случае необходимости обновления, такое обновление производится автоматически (без дополнительного запроса разрешения у пользователя). Без явного указания параметра у пользователя запрашивается разрешение на обновление.</li> </ul> <p><b>Пример команды:</b></p> <pre>sudo Aladdin.EAP.Agent.Terminal server update --allowautoupdate</pre> <p><b>Пример диалога:</b></p> <pre>autotest@freeipa-pre1:~\$ sudo Aladdin.EAP.Agent.Terminal server update Current database version: 4.0.0.30 Actual database version: 4.0.0.30 Updating database is not required.</pre>

Параметр	Описание
	<p>Если после проверки требуется обновление базы данных, то программа сообщит об этом и даст выбор, обновлять ли сейчас базу данных или нет (если только не указан параметр --allowautoupdate).</p> <pre data-bbox="347 369 1185 560"> autotest@fræelipa-orel:~\$ sudo Aladdin.EAP.Agent.Terminal server update Current database version: 4.0.0.29 Actual database version: 4.0.0.30  Updating database is required Backup database before update!  Start update database? [y/n]                     </pre> <p>После нажатия клавиши «n» или любой другой, отличающийся от «y» обновление базы данных будет отменено.</p> <pre data-bbox="347 656 1166 882"> autotest@fræelipa-orel:~\$ sudo Aladdin.EAP.Agent.Terminal server update Current database version: 4.0.0.29 Actual database version: 4.0.0.30  Updating database is required Backup database before update!  Start update database? [y/n] n Update database canceled                     </pre> <p>После нажатия клавиши «y» будет запущено обновление базы данных до актуальной версии.</p> <pre data-bbox="347 949 1217 1258"> Current database version: 4.0.0.29 Actual database version: 4.0.0.30  Updating database is required Backup database before update!  Start update database? [y/n] y Stopping eap-engine... -Добавление поддержки расширенных идентификаторов контейнеров - Finished Update database finished success Starting eap-engine...                     </pre> <p>Если не была передана опция --allowautoupdate, то на моменте запуска сервиса процесс обновления остановится. В противном случае будет выполнена проверка текущего состояния сервера, для чего потребуется ввести логин и пароль пользователя JMS. Затем программа будет ожидать пока сервер изменит свое состояние на рабочее или не истечет время ожидания (2 минуты), если сервер не удалось запустить корректно, то по истечению времени ожидания выведется соответствующая ошибка.</p>
<p><b>autostart</b></p>	<p> <b>Важно!</b> Для своего выполнения команда требует повышения привилегий пользователя с помощью sudo.</p> <p>Используется для управления автостартом сервиса сервера JMS.</p> <p><b>Параметры:</b></p> <ul style="list-style-type: none"> <li>• <b>enable</b> – включение автостарта;</li> <li>• <b>disable</b> – отключение автостарта;</li> </ul> <p><b>Пример команды:</b></p> <pre data-bbox="352 1823 1098 1854"> sudo Aladdin.EAP.Agent.Terminal server autostart enable                     </pre> <pre data-bbox="352 1890 1110 1921"> sudo Aladdin.EAP.Agent.Terminal server autostart disable                     </pre>

Параметр	Описание
<b>runMaintenance</b>	<p>Используется для управления флагом:</p> <p><code>Aladdin.EAP.Agent.Terminal server runMaintenance show</code> – показывает текущее состояние флага</p> <p><code>Aladdin.EAP.Agent.Terminal server runMaintenance allow</code> – разрешает запускать планы обслуживания</p> <p><code>Aladdin.EAP.Agent.Terminal server runMaintenance disallow</code> – запрещает запускать планы обслуживания</p>

## Команда smtp

Настройка подключения к smtp-серверу для отправки email-уведомлений

Параметр	Описание
<b>show</b>	Отображает текущие настройки подключения к smtp-серверу.
<ul style="list-style-type: none"> <li><b>enable</b></li> <li><b>disable</b></li> </ul>	<p>Включает/отключает отправку email-уведомлений.</p> <ul style="list-style-type: none"> <li><b>enable</b> – включение отправки уведомлений;</li> <li><b>disable</b> – отключение отправки уведомлений</li> </ul>
<b>configure</b>	<p>Задаёт настройки подключения к smtp-серверу.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li><b>-h, --host</b> (опциональный) – IP-адрес или полное доменное имя (FQDN) smtp-сервера (почтового сервера, с которого будет осуществляться рассылка), например <code>-h 192.168.3.136</code>;</li> <li><b>-p, --port</b> (опциональный) – порт smtp-сервера (например: <code>-p 25</code>);</li> <li><b>--username</b> (опциональный) – имя учетной записи smtp-сервера, от имени которой будет выполняться отправка email-уведомлений (для тестовых smtp-серверов, таких как <code>smtp4dev</code>, указывать не обязательно);</li> <li><b>--password</b> (опциональный) – пароль пользователя для учетной записи smtp-сервера (см. ключ <code>--username</code>) от имени которой будет выполняться отправка email-уведомлений;</li> <li><b>--ssl</b> (опциональный) – флаг необходимости использования ssl при подключении к smtp-серверу. Допустимые значения: <ul style="list-style-type: none"> <li><code>true</code></li> <li><code>false</code></li> </ul>                     (Например: <code>--ssl false</code>)                      Для включения флага необходимо, чтобы почтовый сервер поддерживал режим StartTLS.</li> <li><b>--from</b> (опциональный) – содержимое поля «from» для отправляемых email-уведомлений (например: <code>--from jms@local.com</code>);   <b>Примечание.</b> Некоторые SMTP-серверы не поддерживают указание отправителя, в этом случае в ключе <code>--from</code> следует указать фактический адрес почтового аккаунта пользователя (то же, значение что и в ключе <code>--username</code>)</li> <li><b>--encoding</b> (опциональный) – кодировка письма. Допустимые значения: <ul style="list-style-type: none"> <li><code>utf-8</code>;</li> <li><code>cp-1252</code>;</li> </ul>                     (Например: <code>--encoding cp-1251</code>)</li> <li><b>--deleteQueue</b> (опциональный) – очищать ли очередь уведомлений при отключенном транспорте (<code>true</code>, <code>false</code>). Опция позволяет удалить «зависшие» уведомления в очереди, которые были сформированы некорректными настройками транспорта.</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal smtp configure -h 192.168.3.136 -p 25 --ssl false --from jms@local.com</pre>

Параметр	Описание
<b>test</b>	Совершает попытку отправить тестовое email-уведомление с текущими настройками подключения к smtp-серверу (см. параметр <b>configure</b> ).

## Команда ssl


### Настройка SSL для административного и клиентского интерфейса

Параметр	Описание
<b>show</b>	<p>Отображает текущую конфигурацию SSL для административного и клиентского интерфейса.</p> <p><b>Например:</b></p> <pre>Aladdin.EAP.Agent.Terminal ssl show</pre> <p><b>Пример выдачи:</b></p> <pre>root@freeipa-orel:/home/autotest# eap-agent ssl show Административный интерфейс (integration):   Адрес: https://*:8128   Отпечаток сертификата: 98CC9CD86245D32DC7ECAC2976DC1F0455280B12 Клиентский интерфейс (client):   Адрес: https://*:8122   Отпечаток сертификата: 98CC9CD86245D32DC7ECAC2976DC1F0455280B12</pre>
<b>enable</b>	<p>Позволяет активировать SSL для административного и/или клиентского интерфейса.</p> <p><b>⚠ Важно!</b> Для своего выполнения команда требует повышения привилегий пользователя с помощью <code>sudo</code>.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>--path</b> – путь к файлу сертификата для SSL</li> <li>• <b>--password</b> – пароль от указанного сертификата</li> <li>• <b>--thumbprint</b> – отпечаток сертификата</li> <li>• <b>--api</b> – тип Api, административный – integration, клиентский – client, оба – all (по умолчанию)</li> </ul> <p>Для активации SSL требуется указать либо путь к файлу сертификата и пароль от контейнера сертификата, либо указать отпечаток уже зарегистрированного в хранилище сертификата.</p> <p><b>Например:</b></p> <pre>Aladdin.EAP.Agent.Terminal ssl enable --path /opt/41/f_pfx/ssl.pfx --password P@ssw0rd</pre>
<b>disable</b>	<p>Позволяет отключить SSL для административного и/или клиентского интерфейса</p> <p><b>⚠ Важно!</b> Для своего выполнения команда требует повышения привилегий пользователя с помощью <code>sudo</code>.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li>• <b>--api</b> – тип Api, административный – integration, клиентский – client, оба – all (по умолчанию)</li> </ul>



## Команда syslog

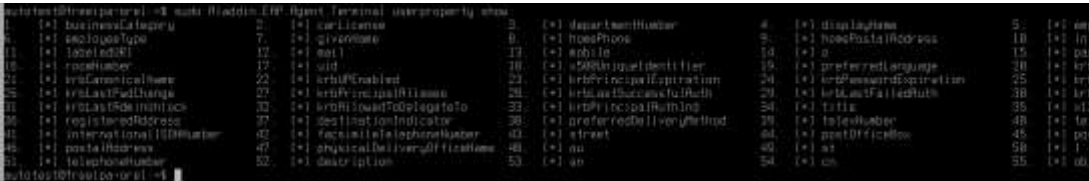
### Настройка регистрации событий на сервере syslog

Параметр	Описание
<b>show</b>	Отображает текущие настройки подключения к syslog-серверу.
<ul style="list-style-type: none"> <li>• <b>enable</b></li> <li>• <b>disable</b></li> </ul>	Включает/отключает регистрацию событий на сервере syslog. <ul style="list-style-type: none"> <li>• <b>enable</b> – включение регистраций;</li> <li>• <b>disable</b> – отключение регистрации</li> </ul>
<b>configure</b>	Задаёт настройки подключения к серверу syslog. <b>Ключи:</b> <ul style="list-style-type: none"> <li>• <b>-h, --host</b> (опциональный) – адрес syslog-сервера (например -h 192.168.3.137);</li> <li>• <b>-p, --port</b> (опциональный) – порт, на котором syslog-сервера «слушает» (например: -p 25);</li> <li>• <b>--ssl</b> (опциональный) – флаг необходимости использования ssl при подключении к syslog-серверу. Допустимые значения:               <ul style="list-style-type: none"> <li>– true</li> <li>– false</li> </ul>               (Например: --ssl false)             </li> <li>• <b>--protocol</b> (опциональный) – протокол отправки. Допустимые значения               <ul style="list-style-type: none"> <li>– TCP или 0 – для использования протокола TCP (использование: <b>--protocol 0</b>),</li> <li>– UDP или 1 – для использования протокола UDP (использование: <b>--protocol 1</b>),</li> </ul> </li> <li>• <b>--appname</b> (опциональный) – текстовый идентификатор приложения (используется в выходных данных Syslog для идентификации приложения). Значение по умолчанию: JMS;</li> <li>• <b>--framing</b> (опциональный) – спецификация Syslog для работы с сервером. Допустимые значения:               <ul style="list-style-type: none"> <li>– OctetCounting или 0 для OctetCounting (RFC5424), использование: <b>--framing 0</b></li> <li>– NonTransparentFraming или 1 для NonTransparentFraming (RFC3164), использование: <b>--framing 1</b>;</li> </ul> </li> </ul> <p> <b>Примечание.</b> Рекомендуется использовать RFC5424, т.к. стандарт RF3164 подразумевает, что сообщение может содержать только печатные символы из таблицы ASCII с кодами в диапазоне от 32 до 126. При выборе RFC3164 невозможна передача кириллицы</p> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal syslog configure -h 192.168.3.136 -p 25 --ssl false -protocol 1 --framing 0</pre>
<b>test</b>	Совершает попытку отправить тестовое сообщение с текущими настройками подключения к серверу syslog (см. параметр <b>configure</b> ).

## Команда userproperty

### Работа с атрибутами пользователя в ресурсной системе

Параметр	Описание
<b>show</b>	Отображает текущую конфигурацию зарегистрированных атрибутов пользователей в ресурсной системе. <b>Ключи:</b>

Параметр	Описание
	<p><b>--accountsystem</b> (опциональный) – имя ресурсной системы; по умолчанию используется имя ресурсной системы указанное в поле [accountSystem] -&gt; name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78)</p> <p><b>Примеры команд:</b></p> <pre>Aladdin.EAP.Agent.Terminal userproperty show --accountsystem DirectoryAlias</pre> <p><b>Пример выдачи:</b></p>  <p>Для обозначения зарегистрированных атрибутов используется символ «*». Идентификаторы атрибутов могут быть использованы в остальных командах управления атрибутами.</p>
<b>register</b>	<p>Регистрирует атрибуты пользователя в ресурсной системы с указанными идентификаторами (см. команду <b>userproperty show</b>) или все поддерживаемые атрибуты (при использовании вместо идентификаторов ключа «all»). Может быть указано несколько идентификаторов через пробел.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li><b>--accountsystem</b> (опциональный) – имя ресурсной системы; по умолчанию используется имя ресурсной системы указанное в поле [accountSystem] -&gt; name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78);</li> <li><b>--properties</b> (обязательный) – идентификаторы атрибутов из команды «show»</li> </ul> <p><b>Примеры команд:</b></p> <pre>Aladdin.EAP.Agent.Terminal userproperty register --accountsystem DirectoryAlias --properties 3 4</pre> <pre>sudo Aladdin.EAP.Agent.Terminal userproperty register --accountsystem DirectoryAlias --properties all</pre> <p>После регистрации атрибутов происходит автоматическая перезагрузка сервера JMS.</p>
<b>unregister</b>	<p>Отменяет регистрацию атрибутов с указанными идентификаторами (см. команду <b>userproperty show</b>). Может быть указано несколько идентификаторов через пробел.</p> <p><b>Ключи:</b></p> <ul style="list-style-type: none"> <li><b>--accountsystem</b> (опциональный) – имя ресурсной системы; по умолчанию используется имя ресурсной системы указанное в поле [accountSystem] -&gt; name файла первоначальной конфигурации (см. «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS», с. 78);</li> <li><b>--properties</b> (обязательный) – идентификаторы атрибутов из команды «show»</li> </ul> <p><b>Пример команды:</b></p> <pre>Aladdin.EAP.Agent.Terminal userproperty unregister --accountsystem freeipa --properties 15 4</pre>

Параметр	Описание
	После отмены регистрации атрибутов происходит автоматическая перезагрузка сервера JMS.

## Приложение 3. Инструкция по сборке расширения rjjava для СУБД PostgreSQL 9.6 под ОС Astra Linux

Для сборки расширения rjjava для для СУБД PostgreSQL 9.6 необходимо выполнить следующие шаги .



**Примечание.** Все команды в данном разделе выполняются в контексте пользователя root. Перед началом работы выполните команду `sudo su -`

1. Убедитесь в установке компонентов СУБД PostgreSQL 9.6 и в их настройке

- postgresql-9.6 (9.6.20-astrace1)
- postgresql-contrib-9.6 (9.6.20-astrace1)

Установите утилиту pgadmin3

2. Актуализируйте операционную среду, выполнив следующие действия.

- 2.1. Откройте на редактирование файл `/etc/apt/sources.list`
- 2.2. Закомментируйте строку, начинающуюся с «deb cdrom» и снимите комментарий со строк, начинающихся с «deb».
- 2.3. Выполните команды:

```
apt update  
apt upgrade
```

3. Установите дополнительные пакеты

- postgresql-common
- postgresql-contrib
- postgresql-server-dev-all
- libssl1.0-dev
- postgresql-server-dev-11
- krb5-multidev
- libkrb5-dev
- g++-8
- g++
- maven
- multiarch-support
- libatk-wrapper-java-jni

Например:

```
apt install postgresql-common postgresql-contrib postgresql-server-dev-all  
libssl1.0-dev postgresql-server-dev-11 krb5-multidev libkrb5-dev g++-8 g++ maven  
multiarch-support libatk-wrapper-java-jni
```

В случае если при установке выявятся ошибки зависимостей, выполните:

```
apt install -f
```

4. Установите пакет openjdk 8.

- 4.1. Загрузите с ресурса <https://packages.debian.org/ru/sid/openjdk-8-jdk> и установите файлы пакета в следующем порядке:

- `dpkg -i libjpeg-turbo8_1.5.2-0ubuntu5_amd64.deb`
- `dpkg -i libjpeg8_8c-2ubuntu8_amd64.deb`
- `dpkg -i openjdk-8-jre-headless_8u162-b12-1_amd64.deb`
- `dpkg -i openjdk-8-jre_8u162-b12-1_amd64.deb`
- `dpkg -i openjdk-8-jdk_8u162-b12-1_amd64.deb`
- `dpkg -i openjdk-8-jdk-headless_8u162-b12-1_amd64.deb`

- 4.2. Поскольку устанавливаемые пакеты автоматически загрузили и установили по умолчанию `openjdk-11`, следует сделать настройку, переключив среду в режим `openjdk-8`. Для этого выполните следующую команду:

```
update-alternatives --config java
```

На предложение интерфейса:

```
Есть 2 варианта для альтернативы java (предоставляет /usr/bin/java).
```

Выбор	Путь	Приор	Состояние
* 0	/usr/lib/jvm/java-11-openjdk-amd64/bin/java	1111	автоматический
режим			
1	/usr/lib/jvm/java-11-openjdk-amd64/bin/java	1111	ручной режим
2	/usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java	1081	ручной режим

```
Press <enter> to keep the current choice[*], or type selection number:
```

Введите «2» (`java-8-openjdk`)

- 4.3. Выполните команду:

```
pg_config
```

5. Выполните компиляцию `pljava-1.5.8`

- 5.1. Выполните команду:

```
apt install git parsec-dev
```

- 5.2. Загрузите исходные файлы `pljava`:

```
git clone https://github.com/tada/pljava.git
```

- 5.3. При возникновении ошибки проверки сертификата или CRL, выполните команды:

```
git config --global http.sslverify false
cd pljava/
git checkout tags/V1_5_8
```

- 5.4. В следующем заголовочном файле

```
sudo nano /usr/include/postgresql/9.6/server/utils/errcodes.h
```

Добавьте строку (выделена красным цветом) если она отсутствовала:

```
#define ERRCODE_INSUFFICIENT_PRIVILEGE_RBT MAKE_SQLSTATE('4','2','5','0','1')
#define ERRCODE_INSUFFICIENT_PRIVILEGE MAKE_SQLSTATE('4','2','5','0','1')
```

- 5.5. Запустите компиляцию:

```
mvn -X -Pwnosign clean install
```

По окончании компиляции должна быть выдача следующего вида:

```

[DEBUG] Installing org.postgresql:pljava-packaging/maven-metadata.xml to /root/.m2
[INFO] Reactor Summary for PostgreSQL PL/Java 1.5.8:
[INFO] PostgreSQL PL/Java ..... SUCCESS [ 1.868 s]
[INFO] PL/Java API ..... SUCCESS [ 3.406 s]
[INFO] PL/Java backend Java code ..... SUCCESS [ 4.237 s]
[INFO] PL/Java backend native code ..... SUCCESS [ 29.515 s]
[INFO] PL/Java Deploy ..... SUCCESS [ 3.438 s]
[INFO] PL/Java Ant tasks ..... SUCCESS [ 5.189 s]
[INFO] PL/Java examples ..... SUCCESS [ 1.314 s]
[INFO] PL/Java packaging ..... SUCCESS [ 2.366 s]
[INFO] BUILD SUCCESS
[INFO] Total time: 52.547 s
[INFO] Finished at: 2023-03-30T08:38:51+03:00

```

Рис. 60 – Фрагмент выдачи после корректной компиляции pljava

Т.е. общий статус всех шагов сборки должен быть Success / «УСПЕШНО»

5.6. Выполните команды:

```
cd pljava-packaging/target/
java -jar ./pljava-pg11.17-amd64-Linux-gpp.jar
```

Версия (выделено красным) может меняться в зависимости от используемой версии СУБД PostgreSQL.

По выполнении команд должно произойти копирование бинарных файлов pljava в директорию Postgres.

Б. Выполните настройку на стороне СУБД PostgreSQL

6.1. Выполните команду

```
sudo -u postgres psql -d <EAPDB>
```

где <EAPDB> – имя БД JMS.

6.2. Из консоли pgAdmin выполните следующие команды:

```
SET pljava.libjvm_location TO '/usr/lib/jvm/java-8-openjdk-
amd64/jre/lib/amd64/server/libjvm.so';

ALTER SYSTEM
SET pljava.libjvm_location TO '/usr/lib/jvm/java-8-openjdk-
amd64/jre/lib/amd64/server/libjvm.so';

SET pljava.classpath TO '/usr/share/postgresql/11/pljava/pljava-1.5.8.jar';

CREATE EXTENSION pljava;
GRANT USAGE ON LANGUAGE JAVA TO public;
GRANT USAGE ON SCHEMA sqlj TO public;
GRANT USAGE ON SCHEMA public TO postgres;
```

Ответы не должны содержать сообщений об ошибках (при корректном выполнении ответы являются краткими).



## Приложение 4. Справочник команд коннектора к Offline Certification Authority

Синтаксис команды:

```
Aladdin.EMS.OfflineCertAuthority <команда> [[<ключ>] [<аргумент>]] ... [[<ключ>] [<аргумент>]]
```

Для получения справки из консоли следует ввести следующую команду:

```
Aladdin.EMS.OfflineCertAuthority --help
```

Ключ --help работает на всех уровнях вложенности команд коннектора (т.е. его можно использовать также после *команды*), например

```
Aladdin.EMS.OfflineCertAuthority initialize --help
```

Полный перечень *команд* и *ключей* коннектора к Offline Certification Authority в Табл. 16.

Табл. 16 – Справочник команд коннектора к Offline Certification Authority

Ключ	Описание
<b>Команда initialize</b>	
Примеры:	
<ul style="list-style-type: none"> <li>инициализация коннектора со всеми параметрами (ключами) по умолчанию:</li> </ul>	
<pre>Aladdin.EMS.OfflineCertAuthority initialize</pre>	
<ul style="list-style-type: none"> <li>инициализация с явно заданными значениями ключей:</li> </ul>	
<pre>Aladdin.EMS.OfflineCertAuthority initialize --controlApiUrl localhost:8119 --eapServiceName eap-engine --logFile '/var/log/aladdin/offline-ca-adapter/OfflineCertAuthorityInitializer.log' --serviceTimeout 00:00:20 --serverTimeout 00:00:30</pre>	
<b>--controlApiUrl</b> либо <b>-u</b>	URL Web API серверного агента, необходимо передать в случае использования в настройках сервера значения отличного от значения по умолчанию (http://localhost:8119)
<b>--eapServiceName</b> либо <b>-n</b>	имя сервиса JMS, по умолчанию eap-engine
<b>--logFile</b> либо <b>-f</b>	путь к файлу с логом установки, по умолчанию /var/log/aladdin/offline-ca-adapter/OfflineCertAuthorityInitializer.log
<b>--serviceTimeout</b>	таймаут обращений к сервису JMS, можно задать в формате ЧЧ:ММ:СС при возникновении каких-либо трудностей в процессе инициализации связанных с таймаутами, по умолчанию 20 секунд
<b>--serverTimeout</b> либо <b>-f</b>	таймаут обращений к серверу JMS, можно задать в формате ЧЧ:ММ:СС при возникновении каких-либо трудностей в процессе инициализации связанных с таймаутами, по умолчанию 30 секунд



Ключ	Описание
<b>--username</b>	Логин для получения доступа к API
<b>--password</b>	Логин для получения доступа к API
<b>--useKerberos</b>	Включение Kerberos-аутентификации. Допустимые значения <ul style="list-style-type: none"><li><b>false</b> (значение по умолчанию)</li><li><b>true</b></li></ul>
<b>--help</b>	Вывод справочной информации о команде
<b>--version</b>	Отображение версии сборки коннектора

## Приложение 5. Справочник команд JMS Web Agent (JWA)

Синтаксис команды:





```
Aladdin.JMS.WebAgent [[<ключ>] [<аргумент>]] ... [[<ключ>] [<аргумент>]]
```

Для получения справки из консоли следует ввести следующую команду:

```
Aladdin.JMS.WebAgent --help
```

Полный перечень *ключей* JWA приведен в Табл. 17.

Табл. 17 – Справочник команд JWA

Ключ	Описание
<p><b>--help</b></p> <p>либо</p> <p><b>-h</b></p>	<p>Вывод справочной информации о команде</p>
<p><b>--jms-host</b></p> <p>либо</p> <p><b>-j</b></p>	<p> <b>Важно!</b> Для выполнения команд с ключом <b>--jms-host</b> требуется повышения привилегий пользователя с помощью <code>sudo</code>.</p> <p>Установка в конфигурационном файле адреса JMS-сервера. Адрес сервера задается в следующем формате:</p> <pre>--jms-host &lt;Сервер_JMS&gt;</pre> <p>где &lt;Сервер_JMS&gt; – FQDN-имя сервера JMS.</p> <p>Например:</p> <pre>sudo Aladdin.JMS.WebAgent --jms-host jmsserver.aladdin.local</pre> <p> <b>Примечание.</b> После выполнения команды с ключом <b>--jms-host</b> для вступления в силу новых параметров следует перезапустить процесс JWA (см. раздел «Управление процессом JWA», с. 27).</p>
<p><b>--jms-web-host</b></p> <p>либо</p> <p><b>-w</b></p> <p>(опциональный параметр)</p>	<p> <b>Важно!</b> Для выполнения команд с ключом <b>--jms-web-host</b> требуется повышения привилегий пользователя с помощью <code>sudo</code>.</p> <p>Установка в конфигурационном файле адреса серверного web-приложения Консоль управления JMS.</p> <p>Адрес сервера задается в следующем формате:</p> <pre>--jms-web-host &lt;Сервер_JMS_Web_Admin&gt;</pre> <p>где &lt;Сервер_JMS_Web_Admin&gt; – FQDN-имя сервера с серверным компонентом Консоль управления JMS.</p> <p>Например:</p> <pre>sudo Aladdin.JMS.WebAgent --jms-web-host jmsserver.aladdin.local</pre> <p> <b>Примечания:</b></p> <ol style="list-style-type: none"> <li>1. После выполнения команды с ключом <b>--jms-web-host</b> для вступления в силу новых параметров следует перезапустить процесс JWA (см. раздел «Управление процессом JWA», с. 27).</li> <li>2. В случае развёртывания JWA на конечных компьютерах пользователей ЛК (т.е. на web-клиенте JWM) допускается данный параметр не указывать, как опциональный</li> </ol>

Ключ	Описание
-v	Отображение версии сборки коннектора

## Приложение 6. Порядок генерации файла `keytab` для прозрачной аутентификации в JMS пользователей из домена AD по протоколу Kerberos

Действия, описанные в данном разделе, производятся на контроллере домена Active Directory (AD) от имени учётной записи с правами администратора домена.

Для генерации файла `keytab` выполните следующие действия.

1. Создайте специальную учётную запись пользователя в домене AD, которая будет использоваться исключительно для получения файла `keytab` и других служебных операций (например, `krbuser`)
2. Добавьте SPN-запись для созданной учётной записи, используя команды

```
setspn -A HTTP/{FQDN_сервера_JMS}@{DNS_имя_домена} {служебная_уч._запись}
setspn -A HOST/{FQDN_сервера_JMS}@{DNS_имя_домена} {служебная_уч._запись}
```

Пример для машины `jmsssv.jms4.local`, домена `jms4.local` и пользователя созданного на первом шаге с именем `krbuser`:

```
setspn -A HTTP/jmsssv.jms4.local@jms4.local krbuser
setspn -A HOST/jmsssv.jms4.local@jms4.local krbuser
```

3. Для проверки корректности выполненной настройки, получите список SPN-записей для указанного пользователя

```
setspn -L {служебная_уч._запись}
```


4. Сгенерируйте файл `keytab` следующей командой:

```
ktpass -out {путь_для_генерируемого_файла} -princ {имя_субъекта_в_узле} -mapuser {служебная_уч._запись} -pass {пароль_для_файла} -pType KRB5_NT_PRINCIPAL -crypto ALL
```

где `{служебная_уч._запись}` -- специальная учётная запись, созданная на первом шаге (`krbuser`)

Например:


```
ktpass -out c:\users\Administrator\Desktop\krb.keytab -princ
HTTP/jmsssv.jms4.local@jms4.local -mapuser krbuser -pass P@ssw0rd -pType
KRB5_NT_PRINCIPAL -crypto ALL
```

 **Примечание.** Для корректной генерации файла `keytab` необходимо, чтобы его пароль соответствовал политике паролей, установленной в домене.

## Приложение 7. Параметры файла первоначальной конфигурации компонентов сервера JWM

### Секция [userplace]

Параметры конфигурирования порталов JWM (секция обязательна для фронтэнда)

Имя настройки	Обязательность наличия	Описание
url	Да	http-адрес JWM-портала (в случае доступа по защищённому каналу -- https)
certificatePath	Нет	Путь к rfx-файлу SSL-ссертификат при доступе по защищённому каналу   <b>Примечание.</b> Сертификат должен содержать поле Subject Name или Subject Alternative Name с DNS name Также необходимо учитывать, что используемый сертификат должен быть доверенным, т.е. все необходимые сертификаты (Root CA и т.д.) должны быть установлены в /usr/local/share/ca-certificates. Это необходимо для проверки цепочки сертификата. Например, в случае использования самоподписанного сертификата, его публичная часть (.crt файл) должна быть в /usr/local/share/ca-certificates.
certificatePassword	Нет	Пароль SSL-сертификата
noValidate	Нет	Флаг отключения проверки валидности сертификата по корневому сертификату и CRL. Допустимые значения <ul style="list-style-type: none"> <li>• true – отключить проверку</li> <li>• false</li> </ul>
dataUrl	Да	Адрес сервиса данных (DatSERVICE) JWM
dataTimeout	Да	Таймаут обращения к сервису данных (в секундах)
dataUseProxy	Да	Флаг использования прокси для обращения к сервису данных. Допустимые значения <ul style="list-style-type: none"> <li>• false</li> <li>• true</li> </ul>
authUrl	Да	Адрес сервиса аутентификации (AuthSERVICE) JWM
authTimeout	Да	Таймаут обращения к сервису аутентификации (в секундах)
authUseProxy	Да	Флаг использования прокси для обращения к сервису аутентификации. Допустимые значения: <ul style="list-style-type: none"> <li>• false</li> <li>• true</li> </ul>

### Секция [jwm]

Настройки режима работы портала (секция обязательна для фронтэнда)

Имя настройки	Обязательность наличия	Описание
mode	Да	Установка режима работы портала. Допустимые значения: <ul style="list-style-type: none"> <li>• Private – установить для внутреннего портала</li> <li>• Public – установить для внешнего портала</li> </ul>
pathBase	Да	Виртуальный каталог. Совместно с адресом хостирования портала формирует URL для обращения

## Секция [cors]

Настройки CORS - если требуется обращение с другого сайта (кросс-серверные запросы) (секция обязательна для фронтэнда)

Имя настройки	Обязательность наличия	Описание
endpoints	Нет	URL-адреса сервисов и порталов для которых разрешено будет совершать кросс-серверные запросы (адреса следует перечислять через «;» без пробелов), например: <code>http://jwmpprivate1.jms4.local:5700;http://jwmservices1.jms4.local:5703;http://jwmpublic1.jms4.local:5699</code>


## Секция [jwa]

URL для поиска JMS Web Agent (секция обязательна для фронтэнда)

Имя настройки	Обязательность наличия	Описание
http	Да	Адрес JWA, например: <code>http://localhost:5601</code>
https	Да	Адрес JWA для обращения по SSL, например: <code>https://localhost:5600</code>


## Секция [dataservice]

Параметры сервиса данных JWM (секция обязательна для бэкэнда)

Имя настройки	Обязательность наличия	Описание
url	Да	Адрес JWM-компонента Dataservice (при доступе по защищённому каналу использовать https) Например: <code>http://jwmservices1.jms4.local:5702</code>
certificatePath	Нет	Путь к pfx-файлу SSL-ссертификат при доступе по защищённому каналу   <b>Примечание.</b> Сертификат должен содержать поле Subject Name или Subject Alternative Name с DNS name Также необходимо учитывать, что используемый сертификат должен быть доверенным, т.е. все необходимые сертификаты (Root CA и т.д.) должны быть установлены в /usr/local/share/ca-certificates. Это необходимо для проверки цепочки сертификата. Например, в случае использования самоподписанного сертификата, его публичная часть (.crt файл) должна быть в /usr/local/share/ca-certificates.
certificatePassword	Нет	Пароль SSL-сертификата
noValidate	Нет	Флаг отключения проверки валидности сертификата по корневому сертификату и CRL. Допустимые значения: <ul style="list-style-type: none"> <li>• true – отключить проверку</li> <li>• false</li> </ul>

### Секция [authservice]

Параметры сервиса аутентификации JWM (секция обязательна для бэкэнда)

Имя настройки	Обязательность наличия	Описание
url	Да	Адрес JWM-компонента Authservice (при доступе по защищённому каналу использовать https) Например: <code>http://jwmservices1.jms4.local:5703</code>
certificatePath	Нет	Путь к rfx-файлу SSL-ссертификат при доступе по защищённому каналу   <b>Примечание.</b> Сертификат должен содержать поле Subject Name или Subject Alternative Name с DNS name Также необходимо учитывать, что используемый сертификат должен быть доверенным, т.е. все необходимые сертификаты (Root CA и т.д.) должны быть установлены в /usr/local/share/ca-certificates. Это необходимо для проверки цепочки сертификата. Например, в случае использования самоподписанного сертификата, его публичная часть (.crt файл) должна быть в /usr/local/share/ca-certificates.
certificatePassword	Нет	Пароль SSL-сертификата
noValidate	Нет	Флаг отключения проверки валидности сертификата по корневому сертификату и CRL. Допустимые значения <ul style="list-style-type: none"> <li>• true – отключить проверку</li> <li>• false</li> </ul>

### Секция [jms]

Параметры подключения к серверу JMS (секция обязательна для бэкэнда)

Имя настройки	Обязательность наличия	Описание
authApiUrl	Да	адрес сервиса аутентификации JMS AuthenticationServiceWebApi (соответствует параметру authenticationManagerUrls ini-файла JMS)
clientApiUrl	Да	адрес сервиса администрирования JMS IntegrationManagerWebApi (соответствует параметру integrationManagerUrls ini-файла JMS)
user	Да	Доменное имя пользователя JMS для обращения к сервису администрирования. Например: <code>jms4\admin</code>
password	Нет	Пароль пользователя JMS для обращения к сервису администрирования.  Указывается, если сертификат JWT не совпадает с сертификатом STS

## Секция [jas]

Параметры подключения к серверу JAS (секция обязательна для бэкэнда)

Имя настройки	Обязательность наличия	Описание
url	Нет	Адрес сервиса аутентификации сервера JAS в следующем формате: <b>http://&lt;FQDN-имя сервера&gt;:8221/api/v4.1</b> где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, jas.devel.corp;

## Секция [database]

Параметры подключения к БД JMS/JAS (секция обязательна для бэкэнда)

Имя настройки	Обязательность наличия	Описание
type	Да	Тип СУБД (например PostgreSQL)
serverAddress	Да	Адрес сервера СУБД
serverPort	Да	Порт сервера СУБД
serverLogin	Да	Серверный логин (имя пользователя от УЗ для СУБД)
serverPassword	Да	Пароль от УЗ для СУБД
databaseName	Да	Имя БД
databaseLogin	Да	Имя пользователя от УЗ для БД
databasePassword	Да	Имя пользователя от УЗ для БД

## Секция [jwt]

Параметры выпуска и проверки JWT-токенов. Общая секция для бэкэнда и фронтэнда (с сертификатом на хосте сервисов (бэкэнде) должен быть связан закрытый ключ. Если указать тот же сертификат, что используется в JMS, пароль пользователя JMS задавать не нужно).

Имя настройки	Обязательность наличия	Описание
certificatePath	Нет	Файл сертификата для импорта, если сертификат ещё не установлен на компьютере. Например: <code>path = /home/admin/install/jwt/cert.pfx</code>
certificatePassword	Нет	Пароль к файлу сертификата для импорта, если сертификат ещё не установлен на компьютере.

Имя настройки	Обязательность наличия	Описание
<b>noValidate</b>	Нет	Флаг отключения проверки валидности сертификата по корневому сертификату и CRL. Допустимые значения <ul style="list-style-type: none"><li>• <b>true</b> – отключить проверку</li><li>• <b>false</b></li></ul>
<b>thumbprint</b>	Нет	Отпечаток ранее установленного на компьютере сертификата
<b>ttl</b>	Да	Время жизни JWT-токена в минутах, влияет на таймаут сессии пользователя.
<b>clockSkew</b>	Да	Допуск времени при проверке JWT-токена, в секундах



## Контакты, техническая поддержка

### Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания «Аладдин Р. Д.».

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40.

Факс: +7 (495) 646-08-82.

E-mail: [aladdin@aladdin.ru](mailto:aladdin@aladdin.ru) (общий).

Web: [www.aladdin.ru](http://www.aladdin.ru)

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

### Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:

**[www.aladdin.ru/support/index.php](http://www.aladdin.ru/support/index.php)**

## Список литературы

- 1 RU.АЛДЕ.03.16.001-05 34 01. Руководство пользователя [Текст]. – «Аладдин Р.Д.»

---

- 2 RU.АЛДЕ.03.16.001-05 32 01-2. Руководство администратора. Часть 2. Функции управления [Текст]. – «Аладдин Р.Д.»

---

- 3 RU.АЛДЕ.03.16.001-05 32 01-3. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS) [Текст]. – «Аладдин Р.Д.» – Файл «JMS-4LX Руководство Администратор 3.docx»

---

- 4 RU.АЛДЕ. 03.16.001-05 30 01-1. Формуляр [Текст]. – «Аладдин Р.Д.»

---

- 5 Единый Клиент JaCarta. Руководство администратора для операционных систем семейства Linux [Текст]. – «Аладдин Р.Д.»

---

- 6 Комплект документации СДР Aladdin LiveOffice
  - Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice. Формуляр. [Текст]. – АО «Аладдин Р.Д.»

---

  - Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice. Руководство по эксплуатации. Часть 1. Руководство администратора. [Текст]. – АО «Аладдин Р.Д.»

---

  - Средство обеспечения безопасной дистанционной работы Aladdin LiveOffice. Руководство по эксплуатации. Часть 2. Руководство пользователя. [Текст]. – АО «Аладдин Р.Д.»

---

- 7 JaCarta Management System. Подготовка и выпуск сертификатов MSCA для JMS [Текст]. – «Аладдин Р.Д.» – Файл JMS\_x.x.x\_Cert\_Guide.docx

## Регистрация изменений

Версия	Изменения
1.01	Добавлено описание поддержки СДР Aladdin LiveOffice.
1.00	Исходная версия документа.

---

## Коротко о компании

Компания «Аладдин Р. Д.» основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

### Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

### Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017  
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17  
Лицензия Министерства обороны РФ № 1384 от 22.08.16  
Система менеджмента качества компании соответствует требованиям  
ГОСТ Р ИСО 9001-2015 (ISO 9001:2015). Сертификат СМК № РОСС RU.ФК14.К00011 от 20.07.18

© АО «Аладдин Р. Д.», 1995–2024. Все права защищены  
Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru